THE GALOIS ACTION AND COHOMOLOGY OF A RELATIVE HOMOLOGY GROUP OF FERMAT CURVES

RACHEL DAVIS, RACHEL PRIES, VESNA STOJANOSKA, AND KIRSTEN WICKELGREN

Abstract. For an odd prime p satisfying Vandiver's conjecture, we give explicit formulae for the action of the absolute Galois group $G_{\mathbb{Q}(\zeta_p)}$ on the homology of the degree p Fermat curve, building on work of Anderson. Further, we study the invariants and the first Galois cohomology group which are associated with obstructions to rational points on the Fermat curve.

1. Introduction

In this paper, we study the action of the absolute Galois group on the homology of the Fermat curve. To describe the first main result, let p be an odd prime, let ζ be a chosen primitive pth root of unity, and consider the cyclotomic field $K = \mathbb{Q}(\zeta)$. Let G_K be the absolute Galois group of K. The Fermat curve of exponent p is the smooth projective curve $X \subset \mathbb{P}^2_K$ of genus $g = (p-1)(p-2)/2$ given by the equation

$$x^p + y^p = z^p.$$

Anderson [And87] proved several foundational results about the Galois module structure of a certain relative homology group of the Fermat curve. These results are closely related to [Iha86] [Col89], and were further developed in [AI88] [And89]. Consider the affine open $U \subset X$ given by $z \neq 0$, which has equation $x^p + y^p = 1$. Consider the closed subscheme $Y \subset U$ defined by $xy = 0$, which consists of $2p$ points. Let $H_1(U, Y; \mathbb{Z}/p)$ denote the étale homology group of the pair $(U \otimes \overline{K}, Y \otimes \overline{K})$; it is a continuous module over $G_{\mathbb{Q}}$. There is a $\mu_p \times \mu_p$ action on X given by

$$(\zeta^i, \zeta^j) \cdot [x, y, z] = [\zeta^i x, \zeta^j y, z],\ (\zeta^i, \zeta^j) \in \mu_p \times \mu_p,$$

which determines an action on U, preserving Y. By [And87, Theorem 6], the group $H_1(U, Y; \mathbb{Z}/p)$ is a free rank one $\mathbb{Z}/p[\mu_p \times \mu_p]$ module, with generator denoted β. The Galois action of $\sigma \in G_K$ is then determined by $\sigma\beta = B_\sigma\beta$, for some unit $B_\sigma \in \mathbb{Z}/p[\mu_p \times \mu_p]$.

Let L be the splitting field of $1 - (1 - x^p)^p$. By [And87, Section 10.5], the G_K action on $H_1(U, Y; \mathbb{Z}/p)$ factors through $\mathrm{Gal}(L/K)$. This implies that the full G_K

We would like to thank BIRS for hosting the WIN3 conference where we began this project. Some of this work was done while the third and fourth authors were in residence at MSRI during the spring 2014 Algebraic topology semester, supported by NSF grant 0932078 000. The second author was supported by NSF grant DMS-15-02227. The third author was supported by NSF grants DMS-1606479 and DMS-1307390. The fourth author was supported by an American Institute of Mathematics five year fellowship and NSF grants DMS-1406380 and DMS-1552730.

module structure of $H_1(U, Y; \mathbb{Z}/p)$ is determined by the finitely many elements B_q for $q \in \mathrm{Gal}(L/K)$.

From Anderson's work, the description of the elements B_q is theoretically complete in the following sense: Anderson shows that B_q is determined by an analogue of the classical gamma function $\Gamma_q \in \overline{\mathbb{F}}_p[\mu_p]$. By [And87, Theorems 7 & 9], there is a formula $B_q = \bar{d}'(\Gamma_q)$ (with $\bar{d}'$ as defined in Section 2.2). The canonical derivation $d : \overline{\mathbb{F}}_p[\mu_p] \to \Omega\overline{\mathbb{F}}_p[\mu_p]$ to the module of Kähler differentials allows one to take the logarithmic derivative $\operatorname{dlog}\Gamma_q$ of Γ_q. Since p is prime, $\operatorname{dlog}\Gamma_q$ determines B_q uniquely [And87, 10.5.2, 10.5.3]. The function $q \mapsto \operatorname{dlog}\Gamma_q$ is in turn determined by a relative homology group of the punctured affine line $H_1(\mathbb{A}^1 - V(\sum_{i=0}^{p-1} x^i), \{0, 1\}; \mathbb{Z}/p)$ [And87, Theorem 10].

In this paper, we determine formulae for B_q for $q \in \mathrm{Gal}(L/K)$ which are explicit enough to be used for applications. We require that p satisfies Vandiver's Conjecture, namely that p does not divide the order h^+ of the class group of $\mathbb{Q}(\zeta + \zeta^{-1})$; this is true for all p less than 163 million and all regular primes. Under this condition, we proved in [DPSW16] that $\mathrm{Gal}(L/K)$ is isomorphic to $(\mathbb{Z}/p)^{r+1}$ where $r = (p-1)/2$. More precisely, let κ denote the classical Kummer map; i.e., for $\theta \in K^*$, let $\kappa(\theta) : G_K \to \mu_p$ be defined by

$$\kappa(\theta)(\sigma) = \frac{\sigma \sqrt[p]{\theta}}{\sqrt[p]{\theta}}.$$

In Section 2.1 we recall that the map

$$\kappa(\epsilon) \times \prod_{i=1}^{\frac{p-1}{2}} \kappa(1 - \epsilon^{-i}) : \mathrm{Gal}(L/K) \to (\mu_p)^{\frac{p+1}{2}}$$

is an isomorphism [DPSW16, Corollary 3.7], and give additional information about the extension $\mathrm{Gal}(L/\mathbb{Q})$.

In Section 2.2, we recall the formula (2.c) for $\operatorname{dlog}\Gamma_q$ from [DPSW16], which uses the above description of $\mathrm{Gal}(L/K)$: Namely, if we write $\operatorname{dlog}\Gamma_q = \sum_{i=1}^{p-1} c_i \epsilon^i \operatorname{dlog}\epsilon$ for c_i in $\mathbb{F}_p$ then the c_i are linear in the coordinate projections of q viewed as an element of $(\mathbb{F}_p)^{\frac{p+1}{2}} \cong (\mu_p)^{\frac{p+1}{2}}$. (There is a chosen root of unity present.) See Equation (2.d). In Section 3, we use this formula to compute B_q explicitly in terms of the generators ϵ_0 and ϵ_1 for $\Lambda_1 = \mathbb{Z}/p[\mu_p \times \mu_p]$. The result is in terms of the truncated exponential maps E_0 and E_1 defined in (3.e) and (3.f) and a polynomial γ defined in (3.g). Although γ has coefficients in $\overline{\mathbb{F}}_p$, the resulting B_q is indeed in Λ_1. Here is the first main result (see Theorem 3.5).

Theorem 1.1. *Suppose p is an odd prime satisfying Vandiver's conjecture. Then the action of* $\mathrm{Gal}(L/K)$ *on the relative homology*

$$H_1(U, Y; \mathbb{Z}/p) \cong \Lambda_1 = \mathbb{Z}/p[\mu_p \times \mu_p]$$

of the Fermat curve is determined as follows. For $q \in \mathrm{Gal}(L/K) \cong (\mathbb{F}_p)^{\frac{p+1}{2}}$, let the image of q in $(\mathbb{F}_p)^{\frac{p+1}{2}}$ be

$$q = (c_0, c_1, \ldots, c_{\frac{p-1}{2}})$$

and for $i > \frac{p-1}{2}$, let c_i be $c_i = c_{p-i} - ic_0$. Let $F \in \bar{\mathbb{F}}_p$ be a solution to the equation

$$F^p - F + \sum_{i=1}^{p-1} c = 0.$$

Let

$$\gamma(\epsilon) = \sum_{i=1}^{p-1} \left(\frac{c_i + c - F}{i} \right) \epsilon^i - \sum_{i=1}^{p-1} \frac{c_i}{i}.$$

Then q acts by multiplication by the element $B_q \in \Lambda_1$ with the explicit formula

$$B_q = \frac{E_0(\gamma(\epsilon_0))E_0(\gamma(\epsilon_1))}{E_0(\gamma(\epsilon_0\epsilon_1))} = \frac{E_1(\gamma_0 + \gamma_1)}{E_0(\gamma_{01})},$$

where E_0 and E_1 are the truncated exponential maps of (3.e) and (3.f), respectively.

A useful corollary of this result is studied in Section 4. Namely, we deduce that the norms of $q \in \mathrm{Gal}(L/K)$ act as zero on $H_1(U, Y; \mathbb{Z}/p)$ almost always: the only exception is when $p = 3$ and q does not fix $\zeta_9 \in L$. See Theorem 4.6.

Having explicitly determined the action of $\mathrm{Gal}(L/K)$, and therefore of G_K on $H_1(U, Y; \mathbb{Z}/p)$, we proceed to studying the zeroth and first associated Galois cohomology groups. Since the action of G_K factors through $\mathrm{Gal}(L/K)$, the G_K-invariants are just the $\mathrm{Gal}(L/K)$-invariants, and we study these in Section 5. Unfortunately, we do not arrive at a general closed-form answer, but we can identify a uniform subspace in Lemmas 5.1 and 5.2, and if Question 5.4 has a positive answer, we can deduce much more from the results in Section 5.2.

In Section 6, we work towards determining the first Galois cohomology group. Initially, the material in this section might seem disjoint from the earlier sections. However, these general results in commutative algebra will eventually play a key role in understanding obstructions for rational points on Fermat curves.

To describe our second main result, consider an extension of finite (or profinite) groups

$$1 \to N \to G \to Q \to 1. \tag{1.a}$$

Suppose M is a $\mathbb{Z}[G]$-module on which N acts trivially. Note that this applies to $G = G_K$, $Q = \mathrm{Gal}(L/K)$, and $M = H_1(U, Y; \mathbb{Z}/p)$. Consider the differential in the spectral sequence associated with (1.a)

$$d_2 : H^1(N, M)^Q \to H^2(Q, M).$$

It gives a short exact sequence

$$0 \to H^1(Q, M) \to H^1(G, M) \to \mathrm{Ker}\, d_2 \to 0,$$

which reduces the calculation of $H^1(G, M)$ to the two simpler calculations of $H^1(Q, M)$ and $\mathrm{Ker}\, d_2$. We address the first of these calculations in Remark 6.5, while the rest of Section 6 concerns the second.

When $Q \simeq (\mathbb{Z}/p)^{r+1}$, we determine the kernel of d_2 algebraically. To state the result about $\mathrm{Ker}(d_2)$, fix a set of generators $\tau_0, \ldots, \tau_r$ of Q. Let $N_{\tau_j} = 1 + \tau_j + \cdots \tau_j^{p-1}$ denote the norm of τ_j. Let $s : Q \to G$ be a set-theoretic section of (1.a). The element $\omega \in H^2(Q, M)$ classifying (1.a) is determined by elements $a_j, c_{j,k} \in N$ where $a_j = s(\tau_j)^p$ for $0 \leq j \leq r$ and where, for $0 \leq j < k \leq r$,

$$c_{j,k} = [s(\tau_k), s(\tau_j)] = s(\tau_k)s(\tau_j)s(\tau_k)^{-1}s(\tau_j)^{-1}.$$

Here is the second main result of this paper (see Theorem 6.11).

Theorem 1.2. *Suppose $\phi \in H^1(N, M)^Q$ is a class represented by a homomorphism $\phi : N \to M$. Then ϕ is in the kernel of d_2 if and only if there exist $m_0, \dots, m_r \in M$ such that*

(1) $\phi(a_j) = -N_{\tau_j} m_j$ for $0 \leq i \leq r$ and

(2) $\phi(c_{j,k}) = (1-\tau_k)m_j - (1-\tau_j)m_k$ for $0 \leq j < k \leq r$.

This theorem is a consequence of the general result about d_2 given in Proposition 6.1, combined with a direct comparison of cocycle representatives coming from two different resolutions which compute $H^*(Q, M)$.

The last section of this paper is disjoint from the main results and is not new, but the methods use new topological tools, and are included for this reason. We recover results about the zeta function mod p of the Fermat curve of exponent p over a finite field of coprime characteristic.

Here is the motivation for studying the first Galois cohomology group of the relative homology $H_1(U, Y; \mathbb{Z}/p)$). Let X be a smooth, proper curve over a number field k and let $\overline{b}$ be a geometric point of X. Let $\pi = \pi_1(X_{\overline{k}}, \overline{b})$ denote the geometric étale fundamental group of X based at $\overline{b}$, and let

$$\pi = [\pi]_1 \supseteq [\pi]_2 \supseteq \ldots \supseteq [\pi]_n \supseteq \ldots$$

denote the lower central series. Let G denote the Galois group of the maximal extension of k ramified only over the primes of bad reduction for X, the infinite places, and a chosen prime p. Using work of Schmidt and Wingberg [SW92], Ellenberg [Ell00] defines a series of obstructions to a point of the Jacobian of a curve X lying in the image of the Abel-Jacobi map. Namely, $X(k)$ and $\operatorname{Jac} X(k)$ can be viewed as subsets of $H^1(G, \pi_p^{\mathrm{ab}})$, where for a nilpotent profinite group, the p-subscript denotes the p-Sylow [Sti13, Chapter 7]. The first of these obstructions

$$\delta_2 : H^1(G, \pi_p^{\mathrm{ab}}) \to H^2(G, ([\pi]_2/[\pi]_3)_p)$$

was also studied by Zarkhin [Zar74]; it is the coboundary map associated to the p-part of the exact sequence

$$0 \to [\pi]_2/[\pi]_3 \to \pi/[\pi]_3 \to \pi/[\pi]_2 \to 0,$$

and has the property that $\operatorname{Ker} \delta_2 \supset X(k)$. Ellenberg's obstructions are related to the non-abelian Chabauty methods of [Kim05] [Kim05] [DCW15] [BDCKW14]. The work of [CNGJ13] gives interesting information related to the embedding $\operatorname{Jac} X(k) \subset H^1(G, \pi_p^{\mathrm{ab}})$ for the Fermat curve.

To pursue this application in the case of Fermat curves, set $M = H_1(U, Y; \mathbb{Z}/p)$ and $Q = \mathrm{Gal}(L/K)$. In future work, we provide information about N (the Galois group of the maximal extension of L ramified only over the prime above p and the infinite places) and the elements $a_j, c_{j,k} \in N$ which classify (1.a).

In the mentioned future work, to apply Theorem 1.2, we need additional information about the elements $B_q \in \mathbb{Z}/p[\mu_p \times \mu_p]$ which we include in Sections 4 - 5. Specifically, we need Theorem 4.6 which states that the norm N_q of B_q is zero for all $q \in Q$ and all $p \geq 5$. We also need Proposition 5.8 about the kernels of $B_{\tau_j} - 1$.

2. Review and extension of previous results

Throughout this paper, p is an odd prime satisfying Vandiver's conjecture.

In our previous paper [DPSW16], we extended results of Anderson [And87] regarding the action of the absolute Galois group of a number field on the first homology of Fermat curves. In this section we briefly summarize and generalize the results we need in the sequel.

The homology group associated to the Fermat curve of exponent p in which one sees the Galois action most transparently is the relative homology group $H_1(U, Y; \mathbb{Z}/p)$. By [And87, Theorem 6], this group is a free rank one module (on a generator called β) over the group ring

$$\Lambda_1 = \mathbb{Z}/p[\mu_p \times \mu_p] = \mathbb{Z}/p[\epsilon_0, \epsilon_1]/\langle \epsilon_i^p - 1 \rangle.$$

Note that Λ_1 itself has an action by $G_{\mathbb{Q}}$, where $g \in G_{\mathbb{Q}}$ acts on both ϵ_0 and ϵ_1 as it does on a primitive p-th root of unity ζ in $K = \mathbb{Q}(\zeta)$. The action of $g \in G_{\mathbb{Q}}$ on $H_1(U, Y; \mathbb{Z}/p)$ is twisted in the sense that

$$g \cdot (f(\epsilon_0, \epsilon_1)\beta) = (g \cdot f(\epsilon_0, \epsilon_1))(g \cdot \beta) = (g \cdot f(\epsilon_0, \epsilon_1))B_g\beta.$$

In particular, if g fixes K, it is easier to describe the action.

Further, by [And87, Section 10.5], if a Galois element fixes the splitting field L of $1 - (1 - x^p)^p$, then it acts trivially on $H_1(U, Y; \mathbb{Z}/p)$. Hence to determine the action of $G_{\mathbb{Q}}$, we are reduced to determining the action of the finite Galois group $\mathrm{Gal}(L/\mathbb{Q})$. To do this explicitly, we need to know the structure of these Galois groups; this is described in the first subsection.

The next subsection introduces the question of determining B_q, where q is an element of the Galois group $Q := \mathrm{Gal}(L/K)$.

2.1. The Galois groups $\mathrm{Gal}(L/K)$ and $\mathrm{Gal}(L/\mathbb{Q})$.

Let $r = \frac{p-1}{2}$; by [DPSW16, Lemma 3.3], the splitting field of L of $1 - (1 - x^p)^p$ is

$$L = K(\sqrt[p]{\zeta}, \sqrt[p]{1 - \zeta^{-i}} | 1 \leq i \leq r).$$

Let $\sigma \in G_K$; for an element θ of K, let $\sqrt[p]{\theta}$ be a choice of a primitive p-root. We define $\kappa(\theta)\sigma$ to be the element of $\mathbb{Z}/p$ such that

$$\sigma \cdot \sqrt[p]{\theta} = \zeta^{\kappa(\theta)\sigma} \sqrt[p]{\theta}.$$

Then $\kappa(\theta)$ defines a homomorphism $G_K \to \mathbb{Z}/p$, which factors through $\mathrm{Gal}(K(\sqrt[p]{\theta})/K)$.

From [DPSW16, Corollary 3.7], the map

$$C = \kappa(\zeta) \times \prod_{i=1}^{r} \kappa(1 - \zeta^{-1}) : \mathrm{Gal}(L/K) \to (\mathbb{Z}/p)^{r+1} \quad (2.b)$$

is an isomorphism. This relationship has a geometric meaning explored further in [DPSW16, Section 4]. We use C to give a convenient basis of $Q = \mathrm{Gal}(L/K)$.

Definition 2.1. For $0 \leq i \leq r$, let τ_i be the inverse image under C of the ith standard basis vector of $(\mathbb{Z}/p)^{r+1}$. In other words, consider the basis for L/K given by $t_0 = \sqrt[p]{\zeta}$ and $t_i = \sqrt[p]{1-\zeta^{-i}}$ for $1 \leq i \leq r$. Then τ_i acts by multiplication by ζ on t_i and acts trivially on t_j for $0 \leq j \leq r$, $j \neq i$.

Now we turn to studying the Galois group $\mathrm{Gal}(L/\mathbb{Q})$; note that $L/\mathbb{Q}$ is itself Galois since L is a splitting field. There is an extension

$$1 \to Q \to \mathrm{Gal}(L/\mathbb{Q}) \to (\mathbb{Z}/p)^* \to 1.$$

Since $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/p)^*$ has order coprime to the order of Q, the Schur-Zassenhaus theorem implies that $\mathrm{Gal}(L/\mathbb{Q})$ splits as a semidirect product of Q and $(\mathbb{Z}/p)^*$. The next result determines this semidirect product.

Lemma 2.2. *The extension $L/\mathbb{Q}$ is Galois with group $Q \rtimes_\psi (\mathbb{Z}/p)^*$ where $\psi : (\mathbb{Z}/p)^* \to \mathrm{Aut}(Q)$ is given by the conjugation action*

$$\psi(a) \cdot \tau_i = \begin{cases} (\tau_{ia})^a, & \text{if } i \neq 0, \\ \tau_0, & \text{if } i = 0. \end{cases}$$

In particular, if a is a generator of $(\mathbb{Z}/p)^*$, then $\psi(a)$ acts transitively on the set of subgroups $\langle \tau_i \rangle$ for $1 \leq i \leq r$.

Proof. We already remarked that $\mathrm{Gal}(L/\mathbb{Q})$ is a semi-direct product $Q \rtimes_\psi (\mathbb{Z}/p)^*$; we just need to determine ψ. For $a \in (\mathbb{Z}/p)^*$, let $\alpha_a \in \mathrm{Aut}(K)$ be given by $\zeta \mapsto \zeta^a$. For the case $i \neq 0$, we need to show

$$\alpha_a \tau_i \alpha_a^{-1}(z) = (\tau_{ia})^a(z), \text{ for all } z \in L, 0 \leq i \leq r.$$

As in Definition 2.1, let $t_j = \sqrt[p]{1-\zeta_p^{-j}}$, for $1 \leq j \leq r$, and $t_0 = \sqrt[p]{\zeta}$. Since t_j, $0 \leq j \leq r$, generate L over K, it suffices to check the above for $z = t_j$.

If $j = ia$, then $(\tau_{ia})^a(t_j) = \zeta^a t_j$ and

$$\alpha_a \tau_i \alpha_a^{-1}(t_{ia}) = \alpha_a \tau_i(t_i) = \alpha_a(\zeta t_i) = \zeta^a t_j.$$

If $j \neq ia$, then t_j is fixed by both $\alpha_a \tau_i \alpha_a^{-1}$ and τ_{ia}.

For the case $i = 0$, we need to show $\alpha_a \tau_0 \alpha_a^{-1}(t_j) = \tau_0(t_j)$, for all $0 \leq j \leq r$. For $j > 0$, t_j is fixed by both τ_0 and $\alpha \tau_0 \alpha^{-1}$. If $j = 0$, then $\tau_0(t_0) = \zeta t_0$ and

$$\alpha_a \tau_0 \alpha_a^{-1}(t_0) = \alpha_a \tau_0(t_0^{a^{-1}}) = \alpha_a(\zeta^{a^{-1}} t_0^{a^{-1}}) = \zeta t_0.$$

□

2.2. **Determining the action of Q on $H_1(U, Y; \mathbb{Z}/p)$.** The action of $q \in Q$ on $H_1(U, Y; \mathbb{Z}/p)$ is determined by a unit B_q of Λ_1, where $\Lambda_1 = \mathbb{Z}/p[\mu_p \times \mu_p] \cong \mathbb{Z}/p[\epsilon_0, \epsilon_1]/\langle \epsilon_i^p - 1 \rangle$. Denote by Λ_0 the group ring $\mathbb{Z}/p[\mu_p] = \mathbb{Z}/p[\epsilon]/\langle \epsilon^p - 1 \rangle$. Let $\bar{\Lambda}_i = \Lambda_i \otimes_{\mathbb{F}_p} \bar{\mathbb{F}}_p$. Define a map $\bar{d}' : \bar{\Lambda}_0^\times \to \bar{\Lambda}_1^\times$ by

$$\bar{d}'(u(\epsilon)) = \frac{u(\epsilon_0)u(\epsilon_1)}{u(\epsilon_0\epsilon_1)}.$$

By [And87, Theorems 7 and 9], B_q is in the image of $\bar{d}'$; in fact, $B_q = \bar{d}'(\Gamma_q)$, where $\Gamma_q \in \bar{\Lambda}_0^\times$ is unique modulo the kernel of $\bar{d}'$, which consists of ϵ^j, $0 \le j \le p-1$. Moreover, for such a Γ_q, if we write $\Gamma_q = \sum_{i=0}^{p-1} d_i \epsilon^i$ with $d_i \in \bar{\mathbb{F}}_p$, then $\sum_{i=0}^{p-1} d_i = 1$ [DPSW16, Lemma 5.4].

The element B_q has several nice properties; it is symmetric under the involution of Λ_1 exchanging ϵ_0 and ϵ_1. Further, $B_q - 1$ is in the ideal $\langle (1-\epsilon_0)(1-\epsilon_1)\rangle$ of Λ_1, which corresponds to the homology group $H_1(U;\mathbb{Z}/p)$ [DPSW16, Lemma 6.1].

As we will see shortly, the image of Γ_q under the logarithmic derivative dlog : $\bar{\Lambda}_0^\times \to \Omega(\bar{\Lambda}_0)$ (to the Kähler differentials on $\bar{\Lambda}_0$) gives us the information needed to determine Γ_q and therefore B_q. Namely, we know from [DPSW16, Corollary 4.2] that, modulo a term in $\bar{\mathbb{F}}_p \operatorname{dlog} \epsilon$,

$$\operatorname{dlog}(\Gamma_q) = \sum_{i=1}^{p-1} c_i \epsilon^i \operatorname{dlog} \epsilon, \tag{2.c}$$

where $c_i = \kappa(1-\zeta^{-i})(q)$. Moreover, (2.b) along with [DPSW16, Corollary 4.4] determines the coefficients c_i from q. Namely, let $c_0 = \kappa(\zeta)(q)$; then $c_0, \ldots c_r$ are determined by the isomorphism C, and for $i > r$,

$$c_i = c_{p-i} - ic_0. \tag{2.d}$$

3. Explicit formula for the action of the Galois group

In this section, we find an explicit formula for B_q for each $q \in Q$, starting with the results summarized in the previous section. This is possible since $\Psi_q := \operatorname{dlog} \Gamma_q$ uniquely determines B_q by [And87, 10.5] (see also [DPSW16, Proposition 5.1]).

3.1. **Truncated exponential maps.** Consider the group ring $\Lambda_0 \cong \mathbb{F}_p[\epsilon]/(\epsilon^p - 1)$; let $y = \epsilon - 1$, so that $\Lambda_0 \cong \mathbb{F}_p[y]/\langle y^p \rangle$. An element $f \in \Lambda_0$ (or $\bar{\Lambda}_0$) can be written uniquely in the form $f = \sum_{i=0}^{p-1} a_i y^i$. Let f_y be the derivative of f with respect to y. Then $f_y(0) = a_1$.

For $f \in y\Lambda_0$ (or $f \in y\bar{\Lambda}_0$), we define an exponential in Λ_0 by

$$E_0(f) = \sum_{i=0}^{p-1} f^i/i!. \tag{3.e}$$

If $f, g \in y\bar{\Lambda}_0$, then $E_0(f)E_0(g) = E_0(f+g)$ and $E_0(f)^{-1} = E_0(-f)$.

Lemma 3.1. *If $f \in y\bar{\Lambda}_0$, then*

$$\operatorname{dlog}(E_0(f)) = (1 + f_y(0)^{p-1} y^{p-1}) df.$$

Proof. Write $f = yg$ and note that $f_y(0) = g(0) = a_1$. Then $f^{p-1} = y^{p-1} a_1^{p-1}$ because $y^p = 0$. So $E_0(-f) f^{p-1} = y^{p-1} a_1^{p-1}$, again because $y^p = 0$. Hence,

$$\begin{aligned}\operatorname{dlog}(E_0(f)) &= E_0(f)^{-1} \frac{dE_0}{df} df = E_0(-f)(E_0(f) - \frac{1}{(p-1)!} f^{p-1}) df \\ &= (1 + E_0(-f) f^{p-1}) df = (1 + f_y(0)^{p-1} y^{p-1}) df.\end{aligned}$$

□

Now we move on to the group ring $\Lambda_1 = \mathbb{F}_p[\mu_p \times \mu_p] \cong \mathbb{F}_p[\epsilon_0, \epsilon_1]/\langle e_i^p - 1\rangle$. Let $y_i = \epsilon_i - 1$, so $\Lambda_1 = \mathbb{F}_p[y_0, y_1]/\langle y_0^p, y_1^p\rangle$.

Let $\mathbb{W}$ denote the Witt vectors over $\mathbb{F}_p$ (respectively $\bar{\mathbb{F}}_p$). Since the characteristic of $\mathbb{W}[\frac{1}{p}]$ is zero, the usual exponential map

$$\exp(f) = \sum_{n=0}^{\infty} \frac{f^n}{n!}$$

is well-defined for $f \in \mathbb{W}[\frac{1}{p}][y_0, y_1]/\langle y_0^p, y_1^p\rangle$.

Lemma 3.2. *If $f \in \langle y_0, y_1\rangle \subset \mathbb{W}[y_0, y_1]/\langle y_0^p, y_1^p\rangle$, then $\exp(f) \in \mathbb{W}[y_0, y_1]/\langle y_0^p, y_1^p\rangle$.*

Proof. It suffices to check that $f^n/n!$ has coefficients in $\mathbb{W}$ for each n. This is clear if $n < p$. If $n \geq p$, write $f = f_0 y_0 + f_1 y_1$ for $f_0, f_1 \in \mathbb{W}[y_0, y_1]/\langle y_0^p, y_1^p\rangle$. Then $f^p = \sum_{i=1}^{p-1} \binom{p}{i} f_0^i f_1^{p-i} y_0^n y_1^{p-i}$. Since $p \mid \binom{p}{i}$ for $1 \leq i \leq p-1$, it follows that $f^p/p!$ has coefficients in $\mathbb{W}$. If $p < n \leq 2p-2$, then $f^n/n! = (f^p/p!) f^{n-p}/((p+1)(p+2)\cdots n)$ and so $f^n/n!$ has coefficients in $\mathbb{W}$. If $n \geq 2p-1$, then $f^n/n! = 0$. $\square$

We now define an exponential E_1 for $f \in \langle y_0, y_1\rangle \subset \Lambda_1$. Let $\tilde{f} \in \mathbb{W}[y_0, y_1]/\langle y_0^p, y_1^p\rangle$ be any lift of f; define

$$E_1(f) = \overline{\exp(\tilde{f})} \tag{3.f}$$

where $\overline{\exp(\tilde{f})}$ denotes the image in Λ_1 (or $\bar{\Lambda}_1$) of $\exp(\tilde{f})$.

Lemma 3.3. *If $f, g \in \langle y_0, y_1\rangle \subset \Lambda_1$ (or $\bar{\Lambda}_1$), then*

(1) $E_1(f)E_1(g) = E_1(f + g)$,

(2) $E_1(f)^{-1} = E_1(-f)$, and

(3) $E_1(f) = \sum_{i=0}^{2p-2} f^i/i!$.

Proof. First, if $f, g \in \mathbb{W}[\frac{1}{p}][y_0, y_1]/\langle y_0^p, y_1^p\rangle$, then $\exp(f + g) = \exp(f)\exp(g)$. By Lemma 3.2, if $f \in \langle y_0, y_1\rangle$, then $\exp(f) \in \mathbb{W}[y_0, y_1]/\langle y_0^p, y_1^p\rangle$. Thus $\exp(f + g)$, $\exp(f)$, and $\exp(g)$ are in $\mathbb{W}[y_0, y_1]/\langle y_0^p, y_1^p\rangle$. Reducing mod p shows that $E_1(f)E_1(g) = E_1(f + g)$.

Next, $E_1(f)$ is invertible because $E_1(f) = 1 + N$ for some element N of the nilradical. Then $E_1(f)^{-1} = E_1(-f)$ because $E_1(f)E_1(-f) = E_1(0) = 1$.

The last statement follows from the fact that $f^{2p-1} = 0$. $\square$

3.2. Γ_q **from** Ψ_q**.** In this subsection, we determine a formula for Γ_q in terms of $\Psi_q = \operatorname{dlog}\Gamma_q$. For convenience, we drop the subscript q, but everything depends on this chosen element of Q.

Proposition 3.4. *Write*

$$\Psi = \sum_{i=1}^{p-1} c_i \epsilon^i \operatorname{dlog}\epsilon,$$

and let $c = \sum_{i=1}^{p-1} c_i$ *be its coefficient sum. Let* $F \in \bar{\mathbb{F}}_p$ *be a solution to the equation* $F^p - F + c = 0$*, and define*

$$\gamma(\epsilon) = \sum_{i=1}^{p-1} \left(\frac{c_i + c - F}{i} \right) \epsilon^i - \sum_{i=1}^{p-1} \frac{c_i}{i}. \tag{3.g}$$

Then

$$\Gamma = E_0(\gamma(\epsilon)).$$

Proof. By (2.c) (and [DPSW16, Corollary 4.2]), $\operatorname{dlog}\Gamma = \Psi$ modulo $\bar{\mathbb{F}}_p \operatorname{dlog}\epsilon$). We rewrite Ψ in the nilpotent basis, i.e.,

$$\Psi = \sum_{i=1}^{p-1} c_i \epsilon^i \operatorname{dlog}\epsilon = \sum_{i=1}^{p-1} c_i (y+1)^{i-1} dy.$$

To find a solution to $\Psi = \operatorname{dlog}(\Gamma)$, we find $f \in y\bar{\Lambda}_0$ such that $\Gamma = E_0(f)$; any unit in Λ_0 is of this form up to scaling.

From the congruence $\binom{p-1}{i} \equiv (-1)^i \bmod p$, it follows that

$$y^{p-1} = ((y+1)-1)^{p-1} = \sum_{i=0}^{p-1} \binom{p-1}{i} (y+1)^i (-1)^{p-1-i} = \sum_{i=0}^{p-1} (y+1)^i. \tag{3.h}$$

By Lemma 3.1,

$$\operatorname{dlog}(E_0(f)) = (1 + f_y(0)^{p-1} y^{p-1}) df = df + f_y(0)^p \left(\sum_{i=0}^{p-1} (y+1)^i \right) dy.$$

Define $f_i \in \bar{\mathbb{F}}_p$ by $f = \sum_{i=0}^{p-1} f_i (y+1)^i$, and note that $f_y(0) = \sum_{i=0}^{p-1} i f_i$. For $1 \le i \le p-1$, we need to solve the equation

$$i f_i + \left(\sum_{i=0}^{p-1} i f_i \right)^p = c_i$$

in such a way that $\sum_{i=0}^{p-1} f_i = 0$. This last condition comes from the fact that $\sum_{i=0}^{p-1} d_i = 1$ if $\Gamma = \sum_{i=0}^{p-1} d_i \epsilon^i$, Section 2.2 (or [DPSW16, Lemma 5.4]).

Adding the first set of equations gives

$$c := \sum_{i=1}^{p-1} c_i = (p-1) \left(\sum_{i=0}^{p-1} i f_i \right)^p + \sum_{i=0}^{p-1} i f_i.$$

Let $F = \sum_{i=0}^{p-1} i f_i$; then F is a solution of $F^p - F + c = 0$. Choose any of the p solutions $F, F+1, \ldots, F+(p-1)$ in $\bar{\mathbb{F}}_p$. Then $f_i = (c_i + c - F)/i$ for $i > 0$ and $f_0 = -\sum_{i>0} f_i = -\sum c_i/i$. ∎

3.3. B_q **from** Ψ_q**.** In this section, we determine a formula for B in terms of Ψ. Let $\gamma_i = \gamma(\epsilon_i)$ for $i = 0, 1$ and let $\gamma_{01} = \gamma(\epsilon_0\epsilon_1)$, where

$$\gamma(\epsilon) = \sum_{i=1}^{p-1} (\frac{c_i + c - F}{i})\epsilon^i - \sum_{i=1}^{p-1} \frac{c_i}{i}.$$

Theorem 3.5. *Suppose p is an odd prime satisfying Vandiver's conjecture. The action of $q \in Q = \mathrm{Gal}(L/K)$ on the relative homology $H_1(U, Y; \mathbb{Z}/p)$ of the Fermat curve is determined by the element $B_q \in \Lambda_1$ with the explicit formula*

$$B_q = \frac{E_0(\gamma_0)E_0(\gamma_1)}{E_0(\gamma_{01})} = \frac{E_1(\gamma_0 + \gamma_1)}{E_1(\gamma_{01}) - T},$$

where T is the "error term"

$$T = E_1(\gamma_{01}) - E_0(\gamma_{01}) = \sum_{i=p}^{2p-2} \frac{\gamma_{01}^i}{i!}.$$

Proof. By [And87, Section 8.4], $B = \Gamma(\epsilon_0)\Gamma(\epsilon_1)/\Gamma(\epsilon_0\epsilon_1)$ in Λ_1. By Proposition 3.4, $\Gamma(\epsilon) = E_0(\gamma(\epsilon))$. If $i = 0, 1$, then $E_0(\gamma_i) = E_1(\gamma_i)$ since $\gamma_i^p = 0$. By Lemma 3.3, $\Gamma(\epsilon_0)\Gamma(\epsilon_1) = E_1(\gamma_0+\gamma_1)$. Since γ_{01}^p is not necessarily zero, the error term T appears in the denominator. □

Remark 3.6. The error term T is in the ideal $\langle y_0, y_1\rangle^p$ since $\gamma_{01} \in \langle y_0, y_1\rangle$.

In the atypical situation that $\gamma_{01}^p = 0$, then $T = 0$ and $B_q = E_1(\gamma_0 + \gamma_1 - \gamma_{01})$.

The next formula follows immediately from Theorem 3.5.

$$B_{q^{-1}} = E_1(\gamma_{01} - \gamma_0 - \gamma_1) - E_1(-\gamma_0 - \gamma_1)T. \tag{3.i}$$

For better display in the next examples, let $x = \epsilon_0 - 1$ and $y = \epsilon_1 - 1$. We arrived at the formulas using Magma; it is difficult to do these calculations by hand.

Example 3.7. *Let $p = 3$. Then $Q = \langle\tau_0, \tau_1\rangle = (\mathbb{Z}/3)^2$.*

If $q = \tau_0$, then $c_0 = 1$, $c_1 = 0$, and $c_2 = 1$; hence $c = 1$. Let F be a solution of $F^3 - F + 1 = 0$, so $f_0 = 1$, $f_1 = 1 - F$, and $f_2 = 1 + F$. Then

$$\gamma_{\tau_0} = 1 + (1 - F)\epsilon + (1 + F)\epsilon^2 = Fy + (1 + F)y^2.$$

After a calculation, one obtains that

$$B_{\tau_0} = 1 + xy + 2xy(x + y).$$

If $q = \tau_1$, then $c_0 = 0$ and $c_1 = c_2 = 1$; hence $c = -1$. Let F be a solution to $F^3 - F - 1 = 0$, so that $f_0 = 0$, $f_1 = -F$, and $f_2 = F$. Then

$$\gamma_{\tau_1} = F(\epsilon^2 - \epsilon) = F(y + y^2),$$

and

$$B_{\tau_1} = 1 + 2xy(x + y) + x^2y^2.$$

Example 3.8. *Let $p = 5$; then $Q = \langle \tau_0, \tau_1, \tau_2 \rangle \simeq (\mathbb{Z}/5)^3$, and we have the following formulas:*

$$\begin{aligned} B_{\tau_0} - 1 &= 4x^4y^4 + x^4y^3 + 3x^4y^2 + 4x^4y + x^3y^4 + x^3y^3 + 2x^3y^2 + 4x^3y \\ &+ 3x^2y^4 + 2x^2y^3 + 3x^2y + 4xy^4 + 4xy^3 + 3xy^2; \\ B_{\tau_1} - 1 &= 2x^4y^4 + 2x^4y^3 + 4x^4y^2 + 4x^4y + 2x^3y^4 + 2x^3y^3 + 4x^3y^2 + x^3y \\ &+ 4x^2y^4 + 4x^2y^3 + x^2y^2 + 4x^2y + 4xy^4 + xy^3 + 4xy^2; \\ B_{\tau_2} - 1 &= 2x^4y^4 + 3x^4y^3 + 3x^4y^2 + 3x^3y^4 + 4x^3y^3 + 4x^3y^2 + 4x^3y \\ &+ 3x^2y^4 + 4x^2y^3 + 4x^2y^2 + x^2y + 4xy^3 + xy^2. \end{aligned}$$

Example 3.9. *Let $p = 7$; then $Q = \langle \tau_0, \tau_1, \tau_2, \tau_3 \rangle \simeq (\mathbb{Z}/7)^4$, and we have:*

$$\begin{aligned} B_{\tau_0} - 1 &= x^6y^5 + 3x^6y^4 + 2x^6y^3 + 2x^6y^2 + 6x^6y \\ &+ x^5y^6 + 2x^5y^5 + x^5y^4 + 4x^5y^3 + 6x^5y \\ &+ 3x^4y^6 + x^4y^5 + 5x^4y^4 + 2x^4y^2 \\ &+ 2x^3y^6 + 4x^3y^5 + 4x^3y^2 + 4x^3y \\ &+ 2x^2y^6 + 2x^2y^4 + 4x^2y^3 + 4x^2y^2 + 3x^2y \\ &+ 6xy^6 + 6xy^5 + 4xy^3 + 3xy^2; \\ B_{\tau_1} - 1 &= 5x^6y^6 + 3x^6y^5 + 2x^6y^4 + 3x^6y^3 + 6x^6y^2 + 6x^6y \\ &+ 3x^5y^6 + 3x^5y^5 + 4x^5y^4 + 4x^5y^3 + 5x^5y^2 + x^5y \\ &+ 2x^4y^6 + 4x^4y^5 + x^4y^4 + 4x^4y^3 + 5x^4y^2 + 6x^4y \\ &+ 3x^3y^6 + 4x^3y^5 + 4x^3y^4 + 2x^3y^3 + 6x^3y^2 + x^3y \\ &+ 6x^2y^6 + 5x^2y^5 + 5x^2y^4 + 6x^2y^3 + x^2y^2 + 6x^2y \\ &+ 6xy^6 + xy^5 + 6xy^4 + xy^3 + 6xy^2; \\ B_{\tau_2} - 1 &= 2x^6y^6 + 6x^6y^5 + 5x^6y^4 + x^6y^3 \\ &+ 6x^5y^6 + x^5y^5 + 5x^5y^4 + 2x^5y^3 + 3x^5y^2 + 6x^5y \\ &+ 5x^4y^6 + 5x^4y^5 + 4x^4y^4 + 5x^4y^2 + 2x^4y \\ &+ x^3y^6 + 2x^3y^5 + 3x^3y^3 + x^3y^2 + 4x^3y \\ &+ 3x^2y^5 + 5x^2y^4 + x^2y^3 + 4x^2y^2 + 3x^2y \\ &+ 6xy^5 + 2xy^4 + 4xy^3 + 3xy^2; \\ B_{\tau_3} - 1 &= 4x^6y^5 + 2x^6y^3 + 4x^6y^2 \\ &+ 4x^5y^6 + 4x^5y^5 + x^5y^4 + 6x^5y^3 + 3x^5y^2 \\ &+ x^4y^5 + 4x^4y^4 + 5x^4y^3 + 4x^4y^2 + 6x^4y \\ &+ 2x^3y^6 + 6x^3y^5 + 5x^3y^4 + 2x^3y^3 + 2x^3y \\ &+ 4x^2y^6 + 3x^2y^5 + 4x^2y^4 + 2x^2y^2 + 5x^2y \\ &+ 6xy^4 + 2xy^3 + 5xy^2. \end{aligned}$$

4. Norm equalities for general primes

For $q \in Q$, consider the unit B_q in $\Lambda_1 = \mathbb{Z}/p[\epsilon_0, \epsilon_1]/\langle \epsilon_i^p - 1 \rangle$. Note that $B_q^p = 1$ since q has order p. In this section, we strengthen this by proving that the norm

$$N_q := 1 + B_q + \cdots + B_q^{p-1}$$

is zero, except in the special case that $p = 3$ and q does not fix $\zeta_9 \in L$.

Throughout this section, it is again more convenient to work with the nilpotent basis of Λ_1 given by $y_i = \epsilon_i - 1$, so that $\Lambda_1 = \mathbb{Z}/p[y_0, y_1]/\langle y_0^p, y_1^p\rangle$.

Before studying the norm of $B = B_q$, we need an auxiliary result. Write

$$\tilde{\gamma} = \gamma_0 + \gamma_1 - \gamma_{01},$$

and note that $\tilde{\gamma} \in \langle y_0, y_1\rangle$, since $\gamma \in \langle y\rangle \subset \bar{\Lambda}_0$.

Proposition 4.1. *If $q \in Q$, then $\tilde{\gamma}$ is in the ideal $\langle y_0, y_1\rangle^2$. If $p \geq 5$, or if $p = 3$ and q fixes $\zeta_9 \in L$, then $\tilde{\gamma}$ is in $\langle y_0, y_1\rangle^3$. More precisely,*

(1) $\tilde{\gamma} = y_0 y_1 \eta$ for some $\eta \in \bar{\Lambda}_1$;

(2) and $\tilde{\gamma} \equiv \alpha y_0 y_1 (y_0 + y_1)$ modulo $\langle y_0, y_1\rangle^4$, for some constant $\alpha \in \mathbb{F}_p$, unless $p = 3$ and $q \notin \langle \tau_1\rangle$.

Proof. For part (1), suppose $\gamma = \sum_{i=0}^{p-1} a_i y^i$. Then

$$\tilde{\gamma} = \gamma(\epsilon_0) + \gamma(\epsilon_1) - \gamma(\epsilon_0\epsilon_1) = \sum_{i=0}^{p-1} a_i (y_0^i + y_1^i) - \sum_{i=0}^{p-1} a_i (y_0 + y_1 + y_0 y_1)^i.$$

Consider the coefficient of y_0^k (equivalently, y_1^k) in

$$\gamma(\epsilon_0\epsilon_1) = \sum_{i=0}^{p-1} a_i (y_0 + y_1(1 + y_0))^i = \sum_{i=0}^{p-1}\sum_{j=0}^{i} a_i \binom{i}{j} y_0^j y_1^{i-j} (1 + y_0)^{i-j}.$$

The monomial y_0^k appears in this sum only when $i = j$, hence also $j = k$, and the coefficient is thus a_j. It follows that the coefficients of y_0^k and y_1^k in $\tilde{\gamma}$ are zero, so $\tilde{\gamma}$ is divisible by $y_0 y_1$.

For part (2), note that $\tilde{\gamma} = y_0 y_1 \eta$, for some $\eta \in \bar{\Lambda}_1$, by part (1). The constant coefficient w of η equals the coefficient of $y_0 y_1$ in $-\gamma_{01}$. Write

$$\gamma = \sum_{i=0}^{p-1} f_i \epsilon^i = \sum_{i=0}^{p-1} f_i (y + 1)^i;$$

then

$$-\gamma_{01} = -\sum_{i=0}^{p-1} f_i (y_0 + 1)^i (y_1 + 1)^i,$$

so it follows that

$$w = -\sum_{i=1}^{p-1} f_i i^2.$$

Since $f_i = \frac{c_i + c - F}{i}$, this simplifies to

$$w = -(c - F)\sum_{i=1}^{p-1} i - \sum_{i=1}^{p-1} i c_i = -\sum_{i=1}^{p-1} i c_i.$$

In particular, this proves that the assignment $\vec{c} = (c_0, c_1, \ldots, c_{p-1}) \to w$ is linear.

Case 1: If $c_0 = 0$ (equivalently, if q fixes ζ_{p^2}), then $c_{p-i} = c_i$. In this case, $w = -\sum_{i=1}^{(p-1)/2} c_i (i + (p - i)) = 0$.

Case 2: Suppose $c_0 = 1$ and $c_i = 0$ for $1 \leq i \leq r = \frac{p-1}{2}$. Then $c_{p-j} = j$ for $1 \leq j \leq r$. So

$$w = -\sum_{i=r+1}^{p-1} i(p-i) = -\sum_{j=1}^{r}(p-j)j = \sum_{j=1}^{r} j^2,$$

and $w = r(r+1)(2r+1)/6$. If $p \geq 5$, then this gives $w = 0$.

General case: Since $\vec{c} \to w$ is linear, the above two cases prove that $w = 0$ for all q when $p \geq 5$. Finally, $\eta \equiv \alpha(y_0 + y_1)$ modulo $\langle y_0, y_1\rangle^2$ since it is symmetric with respect to the involution switching y_0 and y_1. □

The following consequence of Proposition 4.1 will be used in Section 5.

Corollary 4.2. *Suppose $p \geq 5$. Then $B_q - 1$ is in the ideal $\langle y_0, y_1\rangle^3$ for all $q \in Q$. In fact, for some constant $\alpha \in \mathbb{F}_p$, there is a congruence $B_q - 1 \equiv \alpha y_0 y_1(y_0 + y_1)$ modulo $\langle y_0, y_1\rangle^4$.*

Proof. It suffices to show the conclusion for $B_q^{-1} - 1$. By (3.i),

$$B_q^{-1} = E_1(-\tilde{\gamma}) - E_1(-\gamma_0 - \gamma_1)T.$$

Now $T \in \langle y_0, y_1\rangle^p$ by Remark 3.6 so $B_q^{-1} - 1 \equiv E_1(-\tilde{\gamma}) - 1$ modulo $\langle y_0, y_1\rangle^p$. Furthermore, $-\tilde{\gamma} \equiv \alpha y_0 y_1(y_0 + y_1)$ modulo $\langle y_0, y_1\rangle^4$ by Proposition 4.1. Thus $E_1(-\tilde{\gamma}) - 1 = -\tilde{\gamma} + \tilde{\gamma}^2/2 + \cdots \equiv -\tilde{\gamma}$ modulo $\langle y_0, y_1\rangle^8$. Thus $B_q^{-1} - 1 \equiv \alpha y_0 y_1(y_0 + y_1)$ modulo $\langle y_0, y_1\rangle^4$. □

Proposition 4.3. *Let $N_{q^{-1}}$ be the norm of $B_{q^{-1}}$ and $\tilde{\gamma} = \gamma_0 + \gamma_1 - \gamma_{01}$. Then*

$$N_{q^{-1}} = N_{E_1(-\tilde{\gamma})} := \sum_{i=0}^{p-1} E_1(-\tilde{\gamma})^i.$$

Proof. By (3.i), $B_{q^{-1}} = E_1(\gamma_{01} - \gamma_0 - \gamma_1) - E_1(-\gamma_0 - \gamma_1)T$. By Remark 3.6, $T^2 = 0$. Therefore, using Lemma 3.3 repeatedly, we have

$$\begin{aligned} N_{q^{-1}} &= \sum_{m=0}^{p-1} (E_1(-\tilde{\gamma}) - E_1(-\gamma_0 - \gamma_1)T)^m \\ &= \sum_{m=0}^{p-1}\sum_{k=0}^{m}(-1)^k \binom{m}{k} E_1(-(m-k)\tilde{\gamma})E_1(-k(\gamma_0 + \gamma_1))T^k \\ &= \sum_{m=0}^{p-1} E_1(-m\tilde{\gamma}) - \sum_{m=1}^{p-1} mE_1((1-m)\tilde{\gamma} - \gamma_0 - \gamma_1)T \\ &= N_{E_1(-\tilde{\gamma})} - \frac{T}{E_1(\gamma_{01})}\sum_{m=1}^{p-1} mE_1(-m\tilde{\gamma}). \end{aligned}$$

To finish the proof, it suffices to show that the second term in the sum is 0 in Λ_1. By Proposition 4.1, $\tilde{\gamma} \in \langle y_0, y_1\rangle^2$. Since $T \in \langle y_0, y_1\rangle^p$, it suffices to show that

$$S = S(\tilde{\gamma}) = \sum_{m=1}^{p-1} mE_1(-m\tilde{\gamma})$$

is in the ideal $I = \langle y_0, y_1 \rangle^{p-1}$. By Lemma 3.3(3),

$$S = \sum_{m=1}^{p-1} \sum_{t=0}^{2p-2} (-1)^t \frac{m^{t+1}\tilde{\gamma}^t}{t!}.$$

If $t \geq \frac{p-1}{2}$, then $\tilde{\gamma}^t \in I$. Thus, modulo I,

$$S \equiv \sum_{t=0}^{(p-3)/2} (-1)^t \frac{\tilde{\gamma}^t}{t!} (\sum_{m=1}^{p-1} m^{t+1}).$$

However, $\sum_{m=1}^{p-1} m^{t+1} = 0$ when $0 \leq t \leq (p-3)/2$. □

Lemma 4.4. *Suppose $f \in \Lambda_1$ is in the ideal $\langle y_0, y_1 \rangle$. Then*

$$N_{E_1(f)} := \sum_{i=0}^{p-1} E_1(f)^i = f^{p-1} - \frac{f^{2p-2}}{(2p-2)!}.$$

Remark 4.5. Even though it is not possible to divide by p, the expression $\frac{f^{2p-2}}{(2p-2)!}$ is well-defined for $f \in \langle y_0, y_1 \rangle$.

Proof. By Lemma 3.3,

$$N_{E_1(f)} = \sum_{i=0}^{p-1} E_1(f)^i = \sum_{i=0}^{p-1} E_1(if) = 1 + \sum_{i=1}^{p-1} \sum_{m=0}^{2p-2} \frac{i^m f^m}{m!}.$$

Thus

$$N_f = 1 + \sum_{m=0}^{2p-2} \frac{f^m}{m!} \Big(\sum_{i=1}^{p-1} i^m \Big).$$

Recall that, modulo p, $\sum_{i=1}^{p-1} i^m = 0$ unless $m \equiv 0 \bmod p-1$ in which case $\sum_{i=1}^{p-1} i^m = -1$. Also $(p-1)! = -1$. Thus

$$N_{E_1(f)} = 1 - \Big(1 + \frac{f^{p-1}}{(p-1)!} + \frac{f^{2p-2}}{(2p-2)!} \Big) = f^{p-1} - \frac{f^{2p-2}}{(2p-2)!}.$$

□

Theorem 4.6. *For any $q \in Q$, the norm N_q of B_q equals $\tilde{\gamma}^{p-1}$. In particular, $N_q = 0$ for all $q \in Q$ if $p \geq 5$; when $p = 3$, then $N_q = 0$ if q fixes ζ_9.*

Proof. The norm of B_q equals the norm of $B_q^{-1} = B_{q^{-1}}$, which is $N_{q^{-1}}$. By Proposition 4.3, $N_{q^{-1}} = N_{E_1(-\tilde{\gamma})}$, and by Lemma 4.4,

$$N_{E_1(-\tilde{\gamma})} = (-\tilde{\gamma})^{p-1} - \frac{(-\tilde{\gamma})^{2p-2}}{(2p-2)!}.$$

From Proposition 4.1, $\tilde{\gamma}^{2p-2}$ is in the ideal $\langle y_0, y_1 \rangle^{2(2p-2)}$, hence zero. Moreover, by Proposition 4.1(2) if $p \geq 5$, or if q fixes ζ_{p^2}, then $\tilde{\gamma}^{p-1} = 0$. □

Example 4.7. *Let $p = 3$, and $q = \tau_1$; as seen in Example 3.7, $\gamma_{\tau_1} = F(\epsilon^2 - \epsilon)$, so*

$$\tilde{\gamma}_{\tau_1} = F(\epsilon_0^2 - \epsilon_0 + \epsilon_1^2 - \epsilon_1 - \epsilon_0^2\epsilon_1^2 + \epsilon_0\epsilon_1) = -y_0^2 y_1^2 + y_0 y_1 (y_0 + y_1).$$

Thus $\tilde{\gamma}_{\tau_1} \in \langle y_0, y_1 \rangle^3$ and $N_{\tau_1} = \tilde{\gamma}_{\tau_1}^2 = 0$.

Example 4.8. *Let $p = 3$, and $q = \tau_0$; as seen in Example 3.7,*

$$\gamma_{\tau_0} = 1 + (1 - F)\epsilon + (1 + F)\epsilon^2 = Fy + (1 + F)y^2.$$

This implies that

$$\tilde{\gamma}_{\tau_0} = y_0y_1 + (1 + F)y_0y_1(y_0 + y_1 - y_0y_1),$$

showing that $N_{\tau_0} = \tilde{\gamma}_{\tau_0}^2 = y_0^2y_1^2$, which is not zero.

Example 4.9. *Let $p = 5$. Then modulo $\langle y_0, y_1\rangle^4$:*

$$\tilde{\gamma}_{\tau_0} \equiv 3y_0y_1(y_0 + y_1),\ \tilde{\gamma}_{\tau_1} \equiv 4y_0y_1(y_0 + y_1),\ \tilde{\gamma}_{\tau_2} \equiv y_0y_1(y_0 + y_1).$$

5. The Q-invariants

Let M denote the homology group $H_1(U, Y; \mathbb{Z}/p)$, which can be identified with Λ_1. Under this identification, the homology group $H_1(U; \mathbb{Z}/p)$ corresponds to the ideal $\langle(1 - \epsilon_0)(1 - \epsilon_1)\rangle$ [DPSW16, Lemma 6.1]. Recall that $y_i = e_i - 1$.

The Q-invariants of M are

$$M^Q = \{m \in M \mid B_q m = m \text{ for all } q \in Q\}.$$

In Section 5.1, we construct a subspace of M^Q of dimension $2p + 1$ for $p \geq 5$. In Section 5.2, we compare the B_q-invariant subspaces of M for various $q \in Q$.

5.1. A subspace of M^Q.

For $0 \leq k \leq p - 1$, define $\eta_k = \epsilon_1^k \sum_{i=0}^{p-1} \epsilon_0^i$ and $\gamma_k = \epsilon_0^k \sum_{i=0}^{p-1} \epsilon_1^i$. Note that $(1 - \epsilon_0)\eta_k = (1 - \epsilon_1)\gamma_k = 0$.

Lemma 5.1. *Let $L = \langle \eta_k, \gamma_k\rangle_{k=0}^{p-1}$, viewed as a $\mathbb{Z}/p$-subspace of M. Then:*

(1) $\dim(L) = 2p - 1$*;*

(2) $\operatorname{codim}(L \cap H_1(U), L) = 2$*;*

(3) and a basis for L is $\{y_0^{i_0} y_1^{i_1} \mid \text{ at least one of } i_0, i_1 \text{ equals } p - 1\}$.

Proof. (1) The elements η_k for $0 \leq k \leq p - 1$ generate a $\mathbb{Z}/p$-vector space of dimension p. Similarly, γ_k for $0 \leq k \leq p - 1$ generate a $\mathbb{Z}/p$-vector space of dimension p. The intersection $\langle\eta_k\rangle \cap \langle\gamma_k\rangle$ has dimension 1 with basis $\sum_{k=0}^{p-1} \gamma_k = \sum_{k=0}^{p-1} \eta_k$. Thus $\dim(L) = 2p - 1$.

(2) A basis for L is given by η_k for $0 \leq k \leq p - 1$ and γ_k for $0 \leq k \leq p - 2$. Write an element $\xi \in L$ in the form $\xi = A + B$ where $A = \sum_{k=0}^{p-1} a_k\eta_k$ and $B = \sum_{k=0}^{p-2} b_k\gamma_k$.

Since $A \in \langle 1 - \epsilon_0\rangle$, then $\xi \in \langle 1 - \epsilon_0\rangle$ if and only if $B \in \langle 1 - \epsilon_0\rangle$. Since $B = (\sum_{i=0}^{p-1} \epsilon_1^i) \sum_{k=0}^{p-2} b_k\epsilon_0^k$, this condition is satisfied if and only if (i) $\sum_{k=0}^{p-2} b_k = 0$. Similarly, $B \in \langle 1 - \epsilon_1\rangle$, so $\xi \in \langle 1 - \epsilon_1\rangle$ if and only if $A \in \langle 1 - \epsilon_1\rangle$. This condition is satisfied if and only if (ii) $\sum_{k=0}^{p-1} a_k = 0$. Since conditions (i) and (ii) are linearly independent, $\operatorname{codim}(L \cap H_1(U), L) = 2$.

(3) This follows from the fact that $\eta_k = \epsilon_1^k \sum_{i=0}^{p-1} \epsilon_0^i = (y_1 + 1)^k y_0^{p-1}$ and $\gamma_k = \epsilon_0^k \sum_{i=0}^{p-1} \epsilon_1^i = (y_0 + 1)^k y_1^{p-1}$.

□

For $p \geq 5$, let $s_1 = y_0^{p-2} y_1^{p-2}$ and $a_1 = y_0^{p-3} y_1^{p-3}(y_0 - y_1)$.

Lemma 5.2. *The subspace L from Lemma 5.1 is contained in M^Q. If $p = 3$, then $M^Q = L$. If $p \geq 5$, then $s_1, a_1 \in M^Q \cap H_1(U)$, so $\dim(M^Q) \geq 2p + 1$ and $\dim(M^Q \cap H_1(U)) \geq 2p - 1$.*

Proof. To show $L \subset M^Q$, it suffices to show that $(B_q - 1)m = 0$ for each $m \in L$. By Lemma 5.1(3) and symmetry, it suffices to show that $(B_q - 1)y_0^{i_0} y_1^{p-1} = 0$. This is true since $B_q - 1 \in H_1(U) = \langle y_0 y_1 \rangle$ for all $q \in Q$.

By Corollary 4.2, if $p \geq 5$, then $B_q - 1 \equiv \alpha y_0 y_1 (y_0 + y_1) \bmod \langle y_0, y_1 \rangle^4$, for some constant $\alpha \in \mathbb{F}_p$. The given elements s_1 and a_1 annihilate the ideal $\langle y_0, y_1 \rangle^4$; moreover,

$$s_1 y_0 y_1 (y_0 + y_1) = y_0^{p-1} y_1^{p-1} (y_0 + y_1) = 0,$$

and likewise

$$a_1 y_0 y_1 (y_0 + y_1) = y_0^{p-2} y_1^{p-2} (y_0^2 + y_1^2) = 0.$$

□

Remark 5.3. We would be able to say more about M^Q for $p \geq 11$ if the following question has a positive answer.

Question 5.4. Is it true that $\mathrm{Ker}(B_{\tau_i}) = \mathrm{Ker}(B_{\tau_j})$ for all $1 \leq i, j \leq r$? If yes, this would imply that $M^Q = \mathrm{Ker}(B_{\tau_0} - 1) \cap \mathrm{Ker}(B_{\tau_1} - 1)$. Experimentally, the answer is yes when $p = 3, 5, 7$.

Example 5.5. *(1) When $p = 3$, then $L = M^Q = \mathrm{Ker}(B_{\tau_0} - 1) \subset \mathrm{Ker}(B_{\tau_1} - 1)$.*

(2) When $p = 5$, then $M^Q = \mathrm{Span}(L, s_1, a_1)$ As an ideal, M^Q is generated by $\eta_0 = y_0^4$, $\gamma_0 = y_1^4$, and a_1. Also, $\mathrm{Ker}(B_{\tau_i} - 1)$ is the same 13-dimensional subspace for $1 \leq i \leq 4$.

(3) When $p = 7$, then the set $\{s_1, a_1, s_2, a_2\}$ extends a basis of L to a basis of M^Q, where

$$s_2 = y_0^3 y_1^3 (y_0^2 - y_0 y_1 + y_1^2) + y_0^4 y_1^5,$$

$$a_2 = y_0^2 y_1^2 (y_0^3 - y_0^2 y_1 + y_0 y_1^2 - y_1^3) + y_0^3 y_1^4 (y_0 - 2y_1) - y_0^4 y_1^5.$$

Again, $\mathrm{Ker}(B_{\tau_i} - 1)$ is the same 19-dimensional subspace for $1 \leq i \leq 6$.

The following summary of data shows that $M^Q = \mathrm{Span}(L, a_1, s_1)$ when $p = 3, 5$ but not when $p = 7$.

Example 5.6.

p	$\dim(M^Q)$	$\dim(M^Q \cap H_1(U))$
3	5	3
5	11	9
7	17	15

5.2. **A comparison of invariant subspaces for different automorphisms.** Let $B_i = B_{\tau_i}$ where $\tau_1, \dots, \tau_r$ are the chosen generators of Q. Note that $(B_{ia})^a = B_{\tau_{ia}^a}$. Let $\rho_a \in \mathrm{Aut}(M)$ be given by the permutation action $\epsilon_0^i \epsilon_1^j \mapsto \epsilon_0^{ia}\epsilon_1^{ja}$.

The following result does not answer the first part of Question 5.4, but still gives a relation between the kernels of various $(B_i - 1)$.

Lemma 5.7. *Let $a \in (\mathbb{Z}/p)^*$. Then $(B_{ia})^a = \rho_a(B_i)$ for $i \neq 0$ and $B_0 = \rho_a(B_0)$.*

Proof. By Lemma 2.2, we may identify a with an element of $\mathrm{Gal}(L/\mathbb{Q})$. Then

$$a \cdot (B_i\beta) = a \cdot (\tau_i \cdot \beta) = (a\tau_i) \cdot \beta.$$

Consider $a \cdot (B_i\beta)$; recall that B_i is an element of $\Lambda_1 = \mathbb{Z}/p[\mu_p \times \mu_p]$, and the definition of the action of Λ_1 on $H_1(U, Y; \mathbb{Z}/p)$ is via the map $\mu_p \times \mu_p \to \mathrm{Aut}(X)$ given $\epsilon_0^i \times \epsilon_1^j : (x, y) \mapsto (\epsilon_0^i x, \epsilon_1^j y)$. It follows that $a \cdot (B_i\beta) = \rho_a(B_i)(a \cdot \beta)$.

On the other hand, note that $a\tau_i = (a\tau_i a^{-1})a$. By Lemma 2.2, we may identify $(a\tau_i a^{-1})$ with $(\tau_{ia})^a$ when $i \neq 0$, and with τ_0 when $i = 0$. Therefore,

$$\rho_a(B_i)(a \cdot \beta) = \begin{cases} (\tau_{ia})^a \cdot (a \cdot \beta) = B_{ia}^a(a \cdot \beta) & \text{if } i \neq 0 \\ \tau_0 \cdot (a \cdot \beta) = B_0(a \cdot \beta) & \text{if } i = 0 \end{cases}.$$

Because $H_1(U, Y; \mathbb{Z}/p)$ is identified with the Λ_1-orbit of β, there exists an invertible $B'_a \in \Lambda_1$ such that $a \cdot \beta = B'_a\beta$. In the above identification, we can cancel this element and obtain

$$\rho_a(B_i) = \begin{cases} (B_{ia})^a & \text{if } i \neq 0 \\ B_0 & \text{if } i = 0 \end{cases}.$$

□

Proposition 5.8. *If $1 \leq i \leq r$ and $a \in (\mathbb{Z}/p)^*$, then $\mathrm{Ker}(\tau_{ai} - 1) = \rho_a \mathrm{Ker}(\tau_i - 1)$ is an equality of subsets of $H_1(U, Y; \mathbb{Z}/p)$.*

Proof. Since $((B_{ia})^a - 1) = (B_{ai}^{a-1} \dots + B_{ai}^2 + B_{ai} + 1)(B_{ai} - 1)$, it follows that

$$\mathrm{Ker}(B_{ai} - 1) \subseteq \mathrm{Ker}(B_{ai}^a - 1).$$

By Lemma 5.7, $\mathrm{Ker}(B_{ai}^a - 1) = \rho_a \mathrm{Ker}(B_i - 1)$. Thus

$$\mathrm{Ker}(B_{ai} - 1) \subseteq \rho_a \mathrm{Ker}(B_i - 1),$$

and it follows that

$$\mathrm{Ker}(B_i - 1) \subseteq \rho_a \mathrm{Ker}(B_{a^{-1}i} - 1).$$

Applying this equality repeatedly, we conclude

$$\mathrm{Ker}(B_i - 1) \subseteq \rho_a \mathrm{Ker}(B_{a^{-1}i} - 1) \subseteq \rho_a^2 \mathrm{Ker}(B_{a^{-2}i} - 1) \subseteq \dots \subseteq (\rho_a)^j \mathrm{Ker}(B_{a^{-j}i} - 1)$$

for any $j = 1, 2, \dots$. Since $a^{p-1} = 1 \bmod p$, taking $j = p - 1$ allows one to conclude that all of the inclusions are equalities. Thus

$$\mathrm{Ker}(B_{ai} - 1) = \rho_a \mathrm{Ker}(B_i - 1).$$

□

6. Galois cohomology calculations

The goal of this section is to give a method for the efficient computation of the first cohomology group $H^1(G, M)$, where M is the homology group $H_1(U, Y; \mathbb{Z}/p)$, and G is the Galois group of a suitable extension of L over the cyclotomic field $K = \mathbb{Q}(\zeta)$. In future applications, the extension of L will be its maximal extension ramified only over p, or various subextensions of it. As it is difficult to know explicitly the structure of such a group G in general, the direct description of $H^1(G, M)$ in terms of crossed homomorphisms will not give an effective method for computation.

More generally, consider an extension of finite* groups

$$1 \to N \to G \to Q \to 1,$$

and a G-module M. We are interested in determining the first cohomology group $H^1(G, M)$. The Lyndon-Hochschild-Serre spectral sequence gives rise to a long exact sequence

$$0 \to H^1(Q, M^N) \xrightarrow{inf} H^1(G, M) \xrightarrow{res} H^1(N, M)^Q \xrightarrow{d_2} H^2(Q, M^N) \to \dots$$

in which the differential d_2 can be identified with the transgression map [NSW08, 2.4.3], and explicitly constructed as such. Thus the computation of $H^1(G, M)$ reduces to a computation of $H^1(Q, M^N)$, the kernel of the transgression differential d_2, and the extension formed from those two.

We restrict our attention to the case when the normal subgroup N acts trivially on the module M, since our intended application satisfies that assumption.

6.1. **The transgression.** To begin, note that the extension G is determined by its factor set $\omega : Q \times Q \to N$ [Wei94, 6.6.5]. Explicitly, let $s : Q \to G$ be an arbitrary set-theoretic section of the projection $G \to Q$, such that $s(1) = 1$. Then the map

$$\omega(q_1, q_2) = s(q_1)s(q_2)s(q_1q_2)^{-1}, \tag{6.j}$$

is a cocycle, which is independent of the choice of section s when viewed as an element of $H^2(Q, N)$ [Wei94, 6.6.3] or [Bro82, IV.3].

The next proposition is similar to some material in [Sha99, Section 1].

Proposition 6.1. *Let G be an extension of Q by N determined by the factor set ω, and let M be a G-module on which N acts trivially. Then the transgression*

$$d_2 : H^1(N, M)^Q \to H^2(Q, M)$$

is given by

$$d_2(\phi) = -\phi \circ \omega.$$

Proof. By [NSW08, 2.4.3], the transgression in the Hochschild-Serre spectral sequence is given by [NSW08, 1.6.6]. By [Koc02, 3.7 (3.9) and (3.10)], the map defined to be the transgression given in [Koc02, 3.7] coincides with the map given by [NSW08, 1.6.6].

We may thus use the description of the transgression given in [Koc02, 3.7]. Given $\phi : N \to M$ which represents an element in $H^1(N, M)^Q$, we construct an extension

*everything in this section works for profinite groups and continuous cohomology as well

$\tilde{\phi} : G \to M$ as prescribed by [Koc02, 3.7]. Fix the same section $s : Q \to G$ as in the definition of the factor set ω. Since N acts trivially on M, we can choose $\tilde{\phi}(s(q)) = 0$, for any $q \in Q$. Any element $g \in G$ can be written as $g = ns(q)$, with $n \in N, q \in Q$; for this g we define $\tilde{\phi}(g) = \phi(n)$. The transgression $d_2\phi : Q \times Q \to M$ is then given by

$$d_2\phi(q_1, q_2) = \tilde{\phi}(s(q_1)) + s(q_1)\tilde{\phi}(s(q_2)) - \tilde{\phi}(s(q_1)s(q_2)) = -\tilde{\phi}(s(q_1)s(q_2)).$$

Now note that

$$s(q_1)s(q_2) = s(q_1)s(q_2)s(q_1q_2)^{-1}s(q_1q_2) = \omega(q_1, q_2)s(q_1q_2);$$

since $\omega(q_1, q_2)$ is in N, the definition of $\tilde{\phi}$ yields that

$$d_2\phi(q_1, q_2) = -\tilde{\phi}(\omega(q_1, q_2)s(q_1q_2)) = -\phi(\omega(q_1, q_2)).$$

□

6.2. $H^*(Q, M)$**, when** Q **is elementary abelian.** It is well known that the cohomology group $H^1(Q, M)$ consists of crossed homomorphisms $Q \to M$ modulo the principal ones. This description can be seen as coming from the canonical bar resolution of the trivial module $\mathbb{Z}$. For our applications, however, it is also convenient to use the fact that Q is assumed to be elementary abelian of rank $r + 1$ (where $r = \frac{p-1}{2}$), i.e., $Q \cong C_p^{r+1}$, and use the resolution coming from tensoring $(r + 1)$ minimal C_p-resolutions. We will use the resulting chain complex not only for computing $H^1(Q, M)$. More importantly, in the next subsections we will use a comparison between cocycles of these different resolutions in order to obtain a more direct criterion equivalent to Proposition 6.1 in Theorem 6.11 and Corollary 6.12. As we will delve pretty deeply into the inner workings of these resolutions, we start by recalling their constructions.

6.2.1. *The canonical or bar resolution.* For $i \geq 0$, let $B_i = \mathbb{Z}[Q^{i+1}] \cong \mathbb{Z}[Q]^{\otimes(i+1)}$. Then $B_i \simeq \mathbb{Z}[Q] \otimes B_{i-1}$ for $i \geq 1$. Thus, B_i is a free $\mathbb{Z}[Q]$-module generated by elements of the form $[q_1 \otimes \cdots \otimes q_i]$, with each $q_i \in Q$. There is a free resolution

$$B_\bullet = \{\cdots \to B_2 \to B_1 \to B_0\} \to \mathbb{Z}, \tag{6.k}$$

where the differential $d : B_n \to B_{n-1}$ is given by $d = \sum_{i=0}^{n}(-1)^i d_i$, and each d_i is the $\mathbb{Z}[Q]$-equivariant map determined by

$$\begin{aligned} d_0([g_1 \otimes \cdots \otimes g_n]) &= g_1 \cdot [g_2 \otimes \cdots \otimes g_n], \\ d_i([g_1 \otimes \cdots \otimes g_n]) &= [g_1 \otimes \cdots g_i g_{i+1} \cdots \otimes g_n], \text{ for } 1 \leq i \leq n-1, \\ d_n([g_1 \otimes \cdots \otimes g_n]) &= [g_1 \otimes \cdots \otimes g_{n-1}]. \end{aligned}$$

In particular, $d : B_1 \to B_0$ is given by $d([g_1]) = g_1 \cdot [1] - [1]$ and $d : B_2 \to B_1$ is given by $d([g_1 \otimes g_2]) = g_1 \cdot [g_2] - [g_1 g_2] + [g_1]$.

6.2.2. *The tensor complex of minimal* C_p*-resolutions.* Let τ be a generator of C_p; then the complex

$$C_\bullet = \{\cdots \mathbb{Z}[C_p] \xrightarrow{1-\tau} \mathbb{Z}[C_p] \xrightarrow{N_\tau} \mathbb{Z}[C_p] \xrightarrow{1-\tau} \mathbb{Z}[C_p]\} \to \mathbb{Z}$$

is a free resolution of the trivial $\mathbb{Z}[C_p]$-module $\mathbb{Z}$. Now $\mathbb{Z}[Q] \cong \otimes_{j=0}^r \mathbb{Z}[C_p]$. Thus a free resolution of the trivial $\mathbb{Z}[Q]$-module $\mathbb{Z}$ is given by the (totalization of the) tensor complex $\otimes_{j=0}^r C_\bullet$.

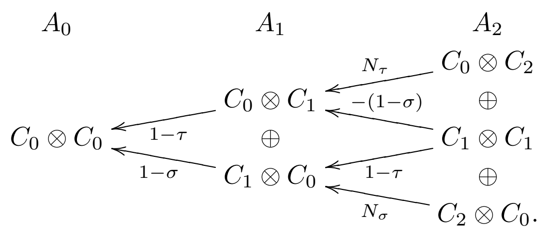
To make this brutally explicit, for $0 \leq j \leq r$, let $C_{\bullet,j}$ denote the same complex as $C_\bullet$ but with the generator of C_p denoted as τ_j. For $i \geq 0$, the ith entry of the complex $C_{\bullet,j}$ is $C_{i,j} \cong \mathbb{Z}[C_p]$, and the map $d_{i,j} : C_{i,j} \to C_{i-1,j}$ is multiplication by $(1-\tau_j)$ if i is odd and multiplication by N_{τ_j} if i is even.

Therefore, $A_\bullet = \mathrm{Tot}(\otimes_{i=0}^r C_\bullet)$ has

$$A_n = \bigoplus_{i_0+\cdots+i_r=n} C_{i_0,0} \otimes \cdots \otimes C_{i_r,r} \cong \bigoplus_{i_0+\cdots+i_r=n} \mathbb{Z}[Q].$$

In particular, $A_0 \cong \mathbb{Z}[Q]$, $A_1 \cong \mathbb{Z}[Q]^{r+1}$, and $A_2 \cong \mathbb{Z}[Q]^\rho$, where the exponent $\rho := r+1+\binom{r+1}{2} = \frac{(p+1)(p+3)}{8}$ is the number of ways to partition 2 into $r+1$ non-negative integers.

We need to define A_1 and A_2 more explicitly in order to describe the differential maps $d : A_1 \to A_0$ and $d : A_2 \to A_1$. Since the notation is elaborate, first consider an example when $p = 3$ and $r = 1$. Let $\sigma = \tau_0$ and $\tau = \tau_1$, then the complex is:



Remark 6.2. Recall that negative signs must be introduced in the totalization of a double complex in order to make the differentials square to zero; see for example [Wei94, p.8].

More generally, recall that A_n is a direct sum of submodules of the form

$$S(\vec{v}) = C_{i_0,0} \otimes \cdots \otimes C_{i_r,r} \cong \mathbb{Z}[Q],$$

where the entries of $\vec{v} = (i_0, \ldots, i_r)$ are non-negative numbers adding up to n. For $n = 1$, define $\vec{v}_j$ to have jth entry 1 and all other entries 0. Then

$$A_1 = \bigoplus_{0 \leq j \leq r} S(\vec{v}_j).$$

For $n = 2$, define $\vec{u}_j$ to have jth entry 1 and all other entries 0; and, for $0 \leq j < k \leq r$, define $\vec{t}_{j,k}$ to have jth entry 1 and kth entry 1 and all other entries 0. Then

$$A_2 = \left(\bigoplus_{0 \leq j \leq r} S(\vec{u}_j) \right) \oplus \left(\bigoplus_{0 \leq j < k \leq r} S(\vec{t}_{j,k}) \right).$$

The following results are now straightforward.

Lemma 6.3. *The differential $d : A_1 \to A_0$ is given by*

$$d(g_0, \ldots, g_r) = \sum_{j=0}^{r} (1 - \tau_j) g_j.$$

Lemma 6.4. *The differential $d : A_2 \to A_1$ is defined using the following maps on the given components (and the zero map everywhere else)*

$$\begin{aligned} d_2 = N_{\tau_j} &\quad : \quad S(\vec{u}_j) \to S(\vec{v}_j), \\ -d_1 = -(1 - \tau_j) &\quad : \quad S(\vec{t}_{j,k}) \to S(\vec{v}_j), \\ d_1 = (1 - \tau_k) &\quad : \quad S(\vec{t}_{j,k}) \to S(\vec{v}_k). \end{aligned}$$

In other words, writing $\alpha \in A_2$ as

$$\alpha = (\oplus_{0 \le j \le r} g_j, \oplus_{0 \le j < k \le r} h_{j,k}),$$

then $d(\alpha) = \oplus_{0 \le j \le r} \beta_j$ where

$$\beta_j = N_{\tau_j} g_j - \sum_{k<j} (1 - \tau_k) h_{k,j} + \sum_{k>j} (1 - \tau_k) h_{j,k}.$$

Again, the negative signs in front of some of the d_1's are because of Remark 6.2.

Remark 6.5. A direct consequence of Lemmas 6.3 and 6.4 is a method for determining $H^1(Q, M)$. Knowing more about the relationships between the kernels and images of $B_i - 1$ as i varies, as in Question 5.4, is likely to give a general result along these lines. Whether or not such questions have useful answers, we used Magma to explicitly calculate $H^1(Q, M)$ when p is small. The dimensions are in this table.

p	$\dim(H^1(Q, M))$
3	9
5	33
7	68

6.2.3. *Comparison of resolutions.* The resolutions $A_\bullet$ and $B_\bullet$ constructed above are both injective resolutions of the trivial Q-module $\mathbb{Z}$. Therefore, by abstract nonsense, there is a map $f_\bullet : A_\bullet \to B_\bullet$, with each $f_i : A_i \to B_i$ being Q-equivariant. The goal of this subsection is to construct f_0, f_1, f_2. In fact, we will take f_0 to be the identity map on $A_0 \cong B_0 = \mathbb{Z}[Q]$. The next two results determine f_1 and f_2 explicitly.

Lemma 6.6. *Define $f_1 : A_1 \to B_1$ by*

$$f_1(g_0, \ldots, g_r) = -\sum_{j=0}^{r} g_j [\tau_j].$$

Then the following diagram commutes

$$\begin{array}{ccc} A_1 & \xrightarrow{d^A} & A_0 \\ {\scriptstyle f_1}\downarrow & & \downarrow{\scriptstyle \mathrm{id}} \\ B_1 & \xrightarrow{d^B} & B_0. \end{array}$$

Proof. Let e_j be the jth standard basis vector. By Lemma 6.3, $\mathrm{id}(d^A(e_j)) = 1 - \tau_j$. By definition $f_1(e_j) = -[\tau_j]$, which equals $d^B(f_1(e_j)) = -(\tau_j - 1)$. Since $\{e_j\}$ generate A_1 as a $\mathbb{Z}[Q]$-module and all the maps are Q-equivariant, the diagram commutes in general. □

Lemma 6.7. *Define $f_2 : A_2 \to B_2$ as follows: for*

$$\alpha = (\oplus_{0 \leq j \leq r} g_j, \oplus_{0 \leq j < k \leq r} h_{j,k}) \in A_2,$$

define

$$f_2(\alpha) = -\sum_{j=0}^{r} g_i[N_{\tau_i} \otimes \tau_i] + \sum_{0 \leq j < k \leq r} h_{j,k}(\tau_k \otimes \tau_j - \tau_j \otimes \tau_k).$$

Then the following diagram commutes

$$\begin{array}{ccc} A_2 & \xrightarrow{d^A} & A_1 \\ {\scriptstyle f_2}\downarrow & & \downarrow{\scriptstyle f_1} \\ B_2 & \xrightarrow{d^B} & B_1. \end{array}$$

Proof. By Lemma 6.4, $d^A(\alpha) = \oplus_{0 \leq j \leq r} \beta_j$ where

$$\beta_j = N_{\tau_j} g_j - \sum_{k<j} (1 - \tau_k) h_{k,j} + \sum_{k>j} (1 - \tau_k) h_{j,k}.$$

Setting $1_j \in A_2$ to be the element such that $g_j = 1$ and all other coordinates are zero, then $f_1(d^A(1_j)) = -N_{\tau_j}[\tau_j]$. By definition, $f_2(1_j) = -[N_{\tau_j} \otimes \tau_j]$. Since $N_{\tau_j}\tau_j = N_{\tau_j}$, it follows that

$$d^B(f_2(1_j)) = -(N_{\tau_j}[\tau_j] - [N_{\tau_j}\tau_j] + [N_{\tau_j}]) = -N_{\tau_j}[\tau_j].$$

Finally, setting $1_{j,k} \in A_2$ to be the element such that $h_{j,k} = 1$ and all other coordinates are zero, then

$$d^A(1_{j,k}) = (1 - \tau_k)e_j - (1 - \tau_j)e_k,$$

and

$$f_1(d^A(1_{j,k})) = f_1((1 - \tau_k)e_j - (1 - \tau_j)e_k) = -(1 - \tau_k)[\tau_j] + (1 - \tau_j)[\tau_k].$$

By definition, $f_2(1_{j,k}) = \tau_k \otimes \tau_j - \tau_j \otimes \tau_k$. Then

$$\begin{aligned} d^B([\tau_k \otimes \tau_j] - [\tau_j \otimes \tau_k]) &= (\tau_k[\tau_j] - [\tau_k\tau_j] + [\tau_k]) - (\tau_j[\tau_k] - [\tau_j\tau_k] + [\tau_j]) \\ &= (\tau_k - 1)[\tau_j] - (\tau_j - 1)[\tau_k]. \end{aligned}$$

Since $\{1_j, 1_{j,k}\}$ generate A_2 as a $\mathbb{Z}[Q]$-module and all the maps are Q-equivariant, the diagram commutes in general. □

6.3. **Comparison of cocycles.** In the above, we constructed two resolutions of the trivial Q-module $\mathbb{Z}$, and explicitly constructed a map between them in low degrees. Now we investigate what this tells us in cohomology. Namely, we know that

$$H^*(Q, M) = \operatorname{Ext}^*_{\mathbb{Z}[Q]}(\mathbb{Z}, M),$$

and the latter can be computed as either $H^* \operatorname{Hom}_{\mathbb{Z}[Q]}(A_\bullet, M)$ or $H^* \operatorname{Hom}_{\mathbb{Z}[Q]}(B_\bullet, M)$. The map $f_\bullet$ gives us a way to compare these two approaches.

Consider a 1-cocycle $a \in H^1(Q, M)$. Let $\phi : Q \to M$ be a bar resolution representative of a, so that the class of ϕ in $H^1(Q, M)$ is a. Then ϕ can be uniquely extended to (and encodes the information of) a $\mathbb{Z}[Q]$-module map $\tilde{\phi} : \mathbb{Z}[Q]^{\otimes 2} \to M$. A representative of a in the $A_\bullet$ resolution is the composition $\psi = \tilde{\phi} \circ f_1$, namely

$$\psi : A_1 \cong \mathbb{Z}[Q]^{r+1} \xrightarrow{f_1} B_1 \cong \mathbb{Z}[Q]^{\otimes 2} \xrightarrow{\tilde{\phi}} M.$$

Now ψ is a $\mathbb{Z}[Q]$-equivariant map determined by its values on the generators e_j of A_1. By Lemma 6.6,

$$m_j := \psi(e_j) = \tilde{\phi}(-[\tau_j]) = -\phi(\tau_j),$$

giving the following result.

Lemma 6.8. *In the resolution* $\operatorname{Hom}_{\mathbb{Z}[Q]}(A_\bullet, M)$*, which starts as*

$$M \to M^{r+1} \to M^\rho \to \cdots,$$

the tuple $(m_0, \ldots, m_r) = (-\phi(\tau_0), \ldots, -\phi(\tau_r)) \in M^{r+1}$ *represents the class* $a \in H^1(Q, M)$ *of the map* $\phi : Q \to M$.

Next, consider a 2-cocycle $b \in H^2(Q, M)$. Let $\varphi : Q \times Q \to M$ represent b. The map φ uniquely determines a $\mathbb{Z}[Q]$-equivariant map $\tilde{\varphi} : B_2 \cong \mathbb{Z}[Q]^{\otimes 3} \to M$. A representative of b in the $A_\bullet$ resolution is the composition

$$\theta : A_2 \cong \mathbb{Z}[Q]^\rho \xrightarrow{f_2} B_2 \xrightarrow{\tilde{\varphi}} M.$$

The map θ is determined by its values on the $\mathbb{Z}[Q]$-generators 1_j and $1_{j,k}$ of A_2. By Lemma 6.7,

$$n_j := \theta(1_j) = \tilde{\varphi}([-N_{\tau_j} \otimes \tau_j]) = -\tilde{\varphi}(N_{\tau_j}, \tau_j) = -\sum_{i=0}^{p-1} \varphi(\tau_j^i, \tau_j),$$
$$n_{j,k} := \theta(1_{j,k}) = \tilde{\varphi}([\tau_k \otimes \tau_j] - [\tau_j \otimes \tau_k]) = \varphi(\tau_k, \tau_j) - \varphi(\tau_j, \tau_k),$$

proving the following result.

Lemma 6.9. *In the resolution* $\operatorname{Hom}_{\mathbb{Z}[Q]}(A_\bullet, M)$*, which starts as*

$$M \to M^{r+1} \to M^\rho \to \cdots,$$

the tuple $(n_j, n_{j,k}) \in M^\rho$ *defined above represents the class* $b \in H^2(Q, M)$ *of the map* $\varphi : Q \times Q \to M$.

6.4. **The kernel of d_2, revisited.** Using the comparison of cocycles from the previous section, we give a more direct description of the kernel of the transgression $d_2 : H^1(N, M)^Q \to H^2(Q, M^N)$ (compared to what Proposition 6.1 implies), when N acts trivially on M and Q is elementary abelian.

We set up some notation associated to the extension

$$1 \to N \to G \to Q \to 1. \tag{6.l}$$

We assume that Q is elementary abelian of rank $(r+1)$; choose generators of Q and denote them by τ_i, with $0 \le i \le r$. To define the factor set ω, we used a section $s : Q \to G$ (and noted that as a cohomology element, ω does not depend on s). Without loss of generality, we can assume not only that $s(1) = 1$, but also

$$s(\tau_0^{t_0} \cdots \tau_r^{t_r}) = s(\tau_0)^{t_0} \cdots s(\tau_r)^{t_r}, \text{ for } 0 \le t_i \le p-1.$$

For $0 \le j \le r$, define elements $a_j \in N$ by

$$a_j = s(\tau_j)^p,$$

and for $0 \le j < k \le r$, define $c_{j,k} \in N$ by

$$c_{j,k} = [s(\tau_k), s(\tau_j)] = s(\tau_k)s(\tau_j)s(\tau_k)^{-1}s(\tau_j)^{-1}.$$

Recall that $\omega : Q \times Q \to N$ was defined as

$$\omega(q_1, q_2) = s(q_1)s(q_2)s(q_1q_2)^{-1}.$$

Elementary calculation then yields the following result.

Lemma 6.10. *If $0 \le j \le r$ and $0 \le t < p-1$, then $\omega(\tau_j^t, \tau_j) = 0$ and $a_j = \omega(\tau_j^{p-1}, \tau_j)$. If $0 \le j < k \le r$, then $c_{j,k} = \omega(\tau_k, \tau_j)\omega(\tau_j, \tau_k)^{-1}$.*

Theorem 6.11. *The class of $\phi : N \to M$ is in the kernel of d_2 if and only if the tuple $(-\phi(a_j), \phi(c_{j,k})) \in M^\rho$ is in the image of the differential in $\mathrm{Hom}_{\mathbb{Z}[Q]}(A_\bullet, M)$,*

$$d^M : M^{r+1} \to M^\rho$$

which is explicitly given by

$$d^M(m_0, \ldots, m_r) = (N_{\tau_j} m_j, -(1-\tau_j)m_k + (1-\tau_k)m_j).$$

Proof. Consider a class in $H^1(N, M)^Q$ represented by a map $\phi : N \to M$. By Proposition 6.1, $\phi \in \mathrm{Ker}(d_2)$ if and only if $\phi \circ \omega : Q \times Q \to M$ represents the zero class in $H^2(Q, M)$. (Note that this is the same as requiring that $-\phi \circ \omega$ represents zero.) This representative is given in the bar resolution, and we now translate the condition on $\phi \circ \omega$ to the $A_\bullet$-resolution as above.

To find a representative for $\phi \circ \omega$ in the $A_\bullet$-resolution, we first extend ω to a Q-equivariant map $\tilde{\omega} : \mathbb{Z}[Q]^3 \to N$ and then take the composition $\tilde{\omega} \circ f_2$. By Lemmas 6.7 and 6.9, $\phi \circ \omega$ is represented by the tuple $(n_j^\phi, n_{j,k}^\phi) \in M^\rho$, where

$$n_j^\phi = \phi(\tilde{\omega}(f_2(1_j))) = \phi(\tilde{\omega}(-N_{\tau_j} \otimes \tau_j)) = -\sum_{i=0}^{p-1} \phi(\omega(\tau_j^i, \tau_j)).$$

By Lemma 6.10,

$$n_j^\phi = -\phi(\omega(\tau_j^{p-1}, \tau_j)) = -\phi(a_j)$$

and

$$n_{j,k}^\phi = \phi(\tilde{\omega}(f_2(1_{j,k}))) = \phi(\tilde{\omega}([\tau_k \otimes \tau_j] - [\tau_j \otimes \tau_k])) = \phi(c_{j,k}).$$

Applying Lemma 6.8 now completes the proof. □

We return now to the situation of the Fermat curve.

Corollary 6.12. *Suppose that E/K is a finite Galois extension dominating L/K. In the extension (6.1), let $Q = \mathrm{Gal}(L/K)$ and $G = \mathrm{Gal}(E/K)$ and $N = \mathrm{Gal}(E/L)$. Recall that N acts trivially on the relative homology $M = H_1(U, Y; A)$.*

Assume $p \geq 5$. Then $\phi : N \to M$ represents an element in the kernel of d_2 if and only if for all $0 \leq j \leq r$,

$$\phi(a_j) = 0,$$

and there is an (r+1)-tuple $(m_0, \ldots m_r) \in M^{r+1}$, such that

$$\phi(c_{j,k}) = -(1 - \tau_j)m_k + (1 - \tau_k)m_j.$$

Proof. This is an immediate application of Theorem 6.11, since N_{τ_i} acts as zero on M by Theorem 4.6. □

Remark 6.13. We have a second more direct proof of Theorem 6.11 as well. The converse direction is long, but we sketch the forward direction here. Note that $-\phi \in \mathrm{Ker}(d_2)$ if and only if the map $\phi \circ \omega : Q \times Q \to M$ represents the zero cohomology class in $H^2(Q, M)$; equivalently, $\phi \circ \omega$ is of the form

$$dm : (q_1, q_2) \mapsto q_1 m(q_2) - m(q_1 q_2) + m(q_1), \tag{6.m}$$

for some map $m : Q \to M$. Let $m_i = m(\tau_i)$.

If $dm = \phi \circ \omega$, then the values $m_j = m(\tau_j) \in M$ determine $m(q)$ for all $q \in Q$ because of the Q-action. Specifically, by induction, one can show $m(\tau_j^{t+1}) = (\sum_{\ell=0}^{t} \tau_j^{\ell}) \cdot m_j$ for $1 \leq t \leq p - 2$. Then $\phi \circ \omega(\tau_j, \tau_j^{p-1}) = \phi(a_j)$. If $\phi \circ \omega = dm$, then $\phi(a_j) = \tau_j \cdot m(\tau_j^{p-1}) + m(\tau_j)$. Thus $-\phi(a_j) = -N_{\tau_j} \cdot m_j$.

Next, if $j < k$, then $m(\tau_j \tau_k) = \tau_j \cdot m_k + m_j$, because $dm(\tau_j, \tau_k) = \omega(\tau_j, \tau_k) = 0$. Recall that $\phi \circ \omega(\tau_k, \tau_j) = \phi(c_{j,k})$. If $\phi \circ \omega = dm$, then $\phi(c_{j,k}) = \tau_k \cdot m_j - m(\tau_j \tau_k) + m_k$, which simplifies to $-\phi(c_{j,k}) = (1 - \tau_k) \cdot m_j - (1 - \tau_j) \cdot m_k$ by substitution.

7. Compatibility with points over finite fields

In this final section, we study the action of Frobenius on schemes defined over a finite field of cardinality ℓ. In Section 7.1, we use motivic homotopy theory to provide congruence conditions on the characteristic polynomials of Frobenius on mod p cohomology. In Section 7.2, we use this and information about B_q to compute the L-polynomial of the degree p Fermat curve modulo p. The results in this section are not new, but they highlight important concepts emerging in the interaction between topology and number theory.

7.1. **Number of points modulo p.** Let X be a smooth, proper scheme over $\mathbb{F}_\ell$. Let F denote the Frobenius morphism. Let p be a prime number not dividing ℓ.

Let N_m denote the number of points of X defined over $\mathbb{F}_{\ell^m}$ for $m \in \mathbb{N}$, and let $\overline{N}_m$ denote the reduction of N_m mod p. By the Lefschetz trace formula, the values N_m are determined by the action of F on $H^*(X_{\overline{\mathbb{F}}_\ell}, \mathbb{Q}_p)$ and the values $\overline{N}_m$ are determined by the action of F on $H^*(X_{\overline{\mathbb{F}}_\ell}, \mathbb{F}_p)$. This section contains a new proof of this fact for $\overline{N}_m$ using realization functors which is made possible by the work of Hoyois [Hoy14].

Define $P_i(t)$ in $\mathbb{Q}_p[t]$ and $\overline{P}_i(t)$ in $\mathbb{F}_p[t]$ by

$$P_i(t) = \det(1 - Ft|H^i(X_{\overline{\mathbb{F}}_\ell}, \mathbb{Q}_p)),\ \overline{P}_i(t) = \det(1 - Ft|H^i(X_{\overline{\mathbb{F}}_\ell}, \mathbb{F}_p)).$$

Define $Z(t)$ in $\mathbb{Q}_p[[t]]$ and $\overline{Z}(t)$ in $\mathbb{F}_p[[t]]$ by

$$Z(t) = \prod_{i=0}^{\infty} P_i(t)^{(-1)^{i+1}},\ \overline{Z}(t) = \prod_{i=0}^{\infty} \overline{P}_i(t)^{(-1)^{i+1}}.$$

If $Q \in \mathbb{F}_p[[t]]$ is invertible (e.g., if $Q(0) = 1$), let $\frac{d}{dt}\log Q = \frac{d}{dt}Q/Q$.

In this section, we prove the following result using motivic homotopy theory.

Proposition 7.1. *The mod p number of points $\overline{N}_m$ of X over $\mathbb{F}_{\ell^m}$ is determined by $\Sigma_{m=1}^{\infty}\overline{N}_m t^{m-1} = \frac{d}{dt}\log \overline{Z}(t)$.*

Proposition 7.1 follows from [Del77, Section 3 Fonctions L Modulo ℓ^n et Modulo p, Theorem 2.2 (b)]. Here is a proof using motivic homotopy theory.

Proof. Let Tr denote the trace of an endomorphism of a strongly dualizable object in a symmetric monoidal category. The Frobenius F is an endomorphism of X viewed as an object the stable $\mathbb{A}^1$-homotopy category of $\mathbb{P}^1$-Spectra over $\mathbb{F}_\ell$. X is strongly dualizable, whence we have $\operatorname{Tr}(F^m)$ in the Grothendieck-Witt ring $\mathrm{GW}(\mathbb{F}_\ell)$. By Hoyois's generalized Lefschetz trace formula [Hoy14, Example 1.6, Theorem 1.3], $\operatorname{Tr}(F^m) = N_m$. Applying the symmetric monoidal functor $H^*((-)_{\overline{\mathbb{F}}_\ell}, \mathbb{F}_p)$, the trace $\operatorname{Tr}(F^m)$ becomes the trace in the symmetric monoidal category of graded $\mathbb{F}_p$ vector spaces, which is $\Sigma_i(-1)^i \operatorname{Tr} F^m|H^i(X_{\overline{\mathbb{F}}_\ell}, \mathbb{F}_p)$. Applying the same functor to the endomorphism N_m of the sphere yields $\overline{N}_m$ regarded as an endomorphism of $\mathbb{F}_p$ viewed as a graded vector space concentrated in degree 0. It follows that

$$\overline{N}_m = \Sigma_i(-1)^i \operatorname{Tr} F^m|H^i(X_{\overline{\mathbb{F}}_\ell}, \mathbb{F}_p). \tag{7.n}$$

The claimed equality then follows from a formal algebraic manipulation. One could apply [Del77, Rapport sur la formula des traces 3.3.1], or to be explicit, proceed as follows.

Since $\overline{P}_i(0) = 1$, it follows that $\overline{P}_i(t) = \prod(1 - a_{i,j}t)$ for some $a_{i,j}$ in $\overline{\mathbb{F}}_p$. Since the matrix corresponding to the action of F on $H^i(X_{\overline{\mathbb{F}}_\ell}, \mathbb{F}_p)$ can be put in upper triangular form over $\overline{\mathbb{F}}_p$, it follows that the diagonal entries are the $a_{i,j}$. Thus $\operatorname{Tr} F^m = \Sigma a_{i,j}^m$ for all m.

Furthermore, $\overline{P}_i$ is invertible in $\mathbb{F}_p[[t]]$ since $\overline{P}_i(0) = 1$. Thus

$$\frac{d}{dt}\log\overline{P}(t) = \frac{\frac{d}{dt}\overline{P}(t)}{\overline{P}(t)} = -\sum_j \frac{a_{i,j}}{1-a_{i,j}t} = -\sum_j\sum_m a_{i,j}^m t^{m-1}.$$

Also,

$$\frac{d}{dt}\log\overline{Z}(t) = \frac{\frac{d}{dt}\overline{Z}(t)}{\overline{Z}(t)}.$$

Since $d/dt\log$ is a homomorphism,

$$\begin{aligned}\frac{d}{dt}\log\overline{Z}(t) &= -\sum_i(-1)^{i+1}\sum_j\sum_m a_{i,j}^m t^{m-1} = \sum_i(-1)^i\sum_m\Big(\sum_j a_{i,j}^m\Big)t^{m-1}\\ &= \sum_i\sum_m(-1)^i\Big(\operatorname{Tr}F^m|H^i(X_{\overline{F}_\ell},\mathbb{F}_p)\Big)t^{m-1}\\ &= \sum_m \overline{N}_m t^{m-1},\end{aligned}$$

where the last equality follows from (7.n). □

7.2. **Application to the Fermat curve.** Let X be the Fermat curve of exponent p over a prime ℓ of $\mathbb{Z}[\zeta_p]$. Let $\mathbb{F}$ be the residue field of ℓ, and $\mathbb{F}_{\ell^m}$ denote the unique degree m extension. Knowledge of B_σ for $\sigma\in Q = \mathrm{Gal}(L/K)$ and Proposition 7.1 determine the zeta function of X modulo p as follows.

Proposition 7.2. *Let X and $\mathbb{F}$ be as above, and let $\operatorname{Jac}X$ denote the Jacobian of X.*

(1) $Z(X/\mathbb{F},T)\equiv(1-T)^{2g-2}\bmod p$. If $N_m := \#X(\mathbb{F}_{\ell^m})$, then $N_m\equiv 0\bmod p$ for all $m\geq 1$.

(2) $Z(\operatorname{Jac}X/\mathbb{F},T)\equiv 1\bmod p$. If $N_m := \#\operatorname{Jac}X(\mathbb{F}_{\ell^m})$, then $N_m\equiv 0\bmod p$ for all $m\geq 1$.

Proof. Note that $Z(Y/\mathbb{F},T)\equiv\overline{Z}(Y/\mathbb{F},T)\bmod p$ for $Y = X$ or $\operatorname{Jac}X$.

(1) The action of the Frobenius F on $M = H_1(U,Y;\mathbb{F}_p)$ is given by multiplication by B_σ, where $\sigma\in Q$ is the Frobenius for ℓ. Now $H_1(X,\mathbb{F}_p)$ is a sub-quotient of M, and M has a basis (namely the nilpotent basis) in which the action of B_σ is lower-triangular with diagonal entries equal to 1. Since $H^1(X,\mathbb{F}_p)$ is the linear dual of $H_1(X,\mathbb{F}_p)$, so it follows that the action of F on $H^1(X,\mathbb{F}_p)$ satisfies $\det(1-FT|H^1(X,\mathbb{F}_p)) = (1-T)^{2g}$, proving the first claim. For the second claim, note that

$$Z(X/\mathbb{F}_q,T)\equiv\frac{(1-T)^{2g}}{(1-T)(1-|\mathbb{F}|T)}\equiv(1-T)^{2g-2}\bmod p,$$

where the last equivalence follows because $\mathbb{F}$ has a pth root of unity, implying $|\mathbb{F}|-1\equiv 0\bmod p$. By Proposition 7.1,

$$\Sigma_{m=1}^\infty\overline{N}_m T^{m-1} = d/dT\log\overline{Z}(T) = -(2g-2)(1-T)^{2g-3}/\overline{Z}(T).$$

But $g = (p-1)(p-2)/2$, so $2g-2 = p^2-3p\equiv 0\bmod p$.

(2) We have seen that the action of F on $H^1(X, \mathbb{F}_p)$ is such that $1 - F$ is nilpotent. Thus the same is true for the action of F on the ith wedge power $\wedge^i H^1(X, \mathbb{F}_p)$. Since $H^i(\mathrm{Jac}\, X, \mathbb{F}_p) \cong \wedge^i H^1(X, \mathbb{F}_p)$, it follows that $\det(1 - FT | H^i(\mathrm{Jac}\, X, \mathbb{F}_p)) = (1-T)^{d_i}$, where $d_i = \binom{2g}{i}$ is the dimension of $\wedge^i H^1(X, \mathbb{F}_p)$. Thus

$$Z(\mathrm{Jac} X/\mathbb{F}_q, T) \equiv (1-T)^{\sum_i (-1)^{i+1} d_i} \equiv 1 \bmod p.$$

□

Remark 7.3. The facts in Proposition 7.2 can also be proven directly. The fact that $N_m \equiv 0 \bmod p$ is a direct consequence of the fact that the $C_p \times C_p$ action on X has 3 orbits of size p and all other orbits of size p^2.

For the fact about the L-polynomial, let χ be a character of $\mathbb{F}$ of order p. Let $J_{(i,j)} = J(\chi^i, \chi^j) \sum_{a+b=1} \chi^i(a)\chi^j(b)$. By [IR90, page 98], $\#X(\mathbb{F}) = L^f + 1 + \sum_S J_{(i,j)}$ where $S = \{(i,j) \mid 1 \leq i,j \leq p-1, \ i+j \not\equiv 0 \bmod p\}$. Note that there are $2g = (p-1)(p-2)$ such pairs. In fact, by [Kat81, page 61], the eigenvalue of Frobenius on the eigenspace of $H^1(X)$ corresponding to (χ^i, χ^j) is $-J_{i,j}$. Lemma 7.2 can also be proven using congruence properties of Jacobi sums and the fact that

$$L(X/\mathbb{F}, T) = \prod_S (1 - J_{(i,j)}T).$$

References

[AI88] Greg Anderson and Yasutaka Ihara, *Pro-l branched coverings of* $\mathbf{P}^1$ *and higher circular l-units*, Ann. of Math. (2) **128** (1988), no. 2, 271–293. MR 960948 1

[And87] Greg W. Anderson, *Torsion points on Fermat Jacobians, roots of circular units and relative singular homology*, Duke Math. J. **54** (1987), no. 2, 501–561. MR 899404 (89g:14012) 1, 2, 5, 7, 10

[And89] ———, *The hyperadelic gamma function*, Invent. Math. **95** (1989), no. 1, 63–131. MR 969414 1

[BDCKW14] Jennifer Balakrishnan, Ishai Dan-Cohen, Minhyong Kim, and Stefan Wewers, *A non-abelian conjecture of birch and swinnerton-dyer type for hyperbolic curves*, November 2014. 4

[Bro82] Kenneth S. Brown, *Cohomology of groups*, Graduate Texts in Mathematics, vol. 87, Springer-Verlag, New York-Berlin, 1982. MR 672956 (83k:20002) 18

[CNGJ13] Phillippe Cassou-Nogués, Jean Gillibert, and Arnaud Jehanne, *Galois module structure and Jacobians of Fermat curves*, January 2013. 4

[Col89] R. F. Coleman, *Anderson-Ihara theory: Gauss sums and circular units*, Algebraic number theory, Adv. Stud. Pure Math., vol. 17, Academic Press, Boston, MA, 1989, pp. 55–72. MR 1097609 (92f:11159) 1

[DCW15] Ishai Dan-Cohen and Stefan Wewers, *Explicit Chabauty-Kim theory for the thrice punctured line in depth 2*, Proc. Lond. Math. Soc. (3) **110** (2015), no. 1, 133–171. MR 3299602 4

[Del77] Pierre Deligne, *Cohomologie étale*, Lecture Notes in Mathematics, Vol. 569, Springer-Verlag, Berlin, 1977, Séminaire de Géométrie Algébrique du Bois-Marie SGA 41øer2, Avec la collaboration de J. F. Boutot, A. Grothendieck, L. Illusie et J. L. Verdier. MR 0463174 (57 #3132) 26

[DPSW16] Rachel Davis, Rachel Pries, Vesna Stojanoska, and Kirsten Wickelgren, *Galois action on the homology of Fermat curves*, to appear in Directions in Number Theory: proceedings of the 2014 WIN3 workshop, published by AWM, 26 pages, http://arxiv.org/abs/1411.4998, 2016. 2, 5, 6, 7, 9, 15

[Ell00] Jordan Ellenberg, *2-nilpotent quotients of fundamental groups of curves*, Preprint, 2000. 4

[Hoy14] Marc Hoyois, *A quadratic refinement of the Grothendieck-Lefschetz-Verdier trace formula*, Algebr. Geom. Topol. **14** (2014), no. 6, 3603–3658. MR 3302973 26

[Iha86] Yasutaka Ihara, *Profinite braid groups, Galois representations and complex multiplications*, Ann. of Math. (2) **123** (1986), no. 1, 43–106. MR 825839 (87c:11055) 1

[IR90] Kenneth Ireland and Michael Rosen, *A classical introduction to modern number theory*, second ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990. MR 1070716 28

[Kat81] Nicholas M. Katz, *Crystalline cohomology, Dieudonné modules, and Jacobi sums*, Automorphic forms, representation theory and arithmetic (Bombay, 1979), Tata Inst. Fund. Res. Studies in Math., vol. 10, Tata Inst. Fundamental Res., Bombay, 1981, pp. 165–246. MR 633662 28

[Kim05] Minhyong Kim, *The motivic fundamental group of* $\mathbf{P}^1 \subset \{0, 1, \infty\}$ *and the theorem of Siegel*, Invent. Math. **161** (2005), no. 3, 629–656. MR 2181717 4

[Koc02] Helmut Koch, *Galois theory of p-extensions*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002, With a foreword by I. R. Shafarevich, Translated from the 1970 German original by Franz Lemmermeyer, With a postscript by the author and Lemmermeyer. MR 1930372 18, 19

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, second ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2008. MR 2392026 18

[Sha99] Romyar Thomas Sharifi, *Twisted Heisenberg representations and local conductors*, ProQuest LLC, Ann Arbor, MI, 1999, Thesis (Ph.D.)–The University of Chicago. MR 2716836 18

[Sti13] Jakob Stix, *Rational points and arithmetic of fundamental groups*, Lecture Notes in Mathematics, vol. 2054, Springer, Heidelberg, 2013, Evidence for the section conjecture. MR 2977471 4

[SW92] Alexander Schmidt and Kay Wingberg, *On the fundamental group of a smooth arithmetic surface*, Math. Nachr. **159** (1992), 19–36. MR 1237099 (94k:14026) 4

[Wei94] Charles A. Weibel, *An introduction to homological algebra*, Cambridge Studies in Advanced Mathematics, vol. 38, Cambridge University Press, Cambridge, 1994. MR 1269324 18, 20

[Zar74] Ju. G. Zarhin, *Noncommutative cohomology and Mumford groups*, Mat. Zametki **15** (1974), 415–419. MR 0354612 (50 #7090) 4

University of Wisconsin-Madison

E-mail address: rachel.davis@wisc.edu

Colorado State University

E-mail address: pries@math.colostate.edu

University of Illinois at Urbana-Champaign

E-mail address: vesna@illinois.edu

Georgia Institute of Technology

E-mail address: kwickelgren3@math.gatech.edu